

网络入侵检测用户手册

目 录

1 文档介绍.....	1
1.1. 文档目的.....	1
1.2. 文档范围.....	1
1.3. 读者对象.....	错误！未定义书签。
1.4. 参考文档.....	错误！未定义书签。
1.5. 术语与缩写解释.....	错误！未定义书签。
2. 系统概述	1
3. 运行环境	2
3.1. 硬件.....	2
3.2. 软件.....	2
3.3. 网络.....	2
4. 安装	2
5. 启动	2
5.1. 管理端的启动.....	3
6. Insight 管理端使用说明	3
6.1. 操作界面概述.....	3
6.2. 用户登录.....	4
6.2.1 操作步骤	5
6.2.2 异常处理	5
6.3. 实时监控安全事件.....	5

6.3.1设置安全事件等级	6
6.3.2安全事件邮件转发	6
6.3.3查看安全事件	7
6.3.4确认安全事件	8
6.3.5关闭安全事件	8
6.3.6关联安全事件	8
6.3.7查看关联安全事件	9
6.3.8查看经验库	10
6.3.9添加处理记录	11
6.3.10查看处理记录	12
6.3.11查看攻击手段场景	13
6.3.12查看原始入侵行为	14
6.3.13发送通知类消息	15
6.3.14发送控制类消息	16
6.3.15查看运行状态	17
6.3.16查看配置信息	18
6.3.17查看设备信息	19
6.3.18查看流量信息	20
6.3.19查看相关的安全事件	21
6.4. 查询安全事件	22
6.4.1描述	22
6.4.2进入方式	22
6.4.3操作步骤	22
6.4.4相关操作	22
6.4.5异常处理	22
6.4.6输入数据	23
6.4.7输出数据	23
6.4.8操作举例	23
6.5. 查看安全事件数量报告	24
6.5.1描述	24
6.5.2进入方式	24
6.5.3操作步骤	24
6.5.4相关操作	25
6.5.5异常处理	25
6.5.6输入数据	25
6.5.7输出数据	25
6.5.8操作举例	25
6.6. 查看安全事件等级报告	26

6.6.1描述	26
6.6.2进入方式	26
6.6.3操作步骤	26
6.6.4相关操作	26
6.6.5异常处理	27
6.6.6输入数据	27
6.6.7输出数据	27
6.6.8操作举例	27
6.7. 查看安全事件状态报告	28
6.7.1描述	28
6.7.2进入方式	28
6.7.3操作步骤	28
6.7.4相关操作	29
6.7.5异常处理	29
6.7.6输入数据	29
6.7.7输出数据	29
6.7.8操作举例	29
6.8. 查询入侵行为	30
6.8.1描述	30
6.8.2进入方式	30
6.8.3操作步骤	30
6.8.4相关操作	30
6.8.5异常处理	31
6.8.6输入数据	31
6.8.7输出数据	31
6.8.8操作举例	32
6.9. 查看入侵行为数量报告	32
6.9.1描述	32
6.9.2进入方式	32
6.9.3操作步骤	33
6.9.4相关操作	33
6.9.5异常处理	33
6.9.6输入数据	33
6.9.7输出数据	33
6.9.8操作举例	33
6.10. 查看入侵行为等级分析报告	34

6.10.1描述	34
6.10.2进入方式	34
6.10.3操作步骤	34
6.10.4相关操作	35
6.10.5异常处理	35
6.10.6输入数据	35
6.10.7输出数据	35
6.10.8操作举例	35
6.11. 查看入侵手段分布报告	36
6.11.1描述	36
6.11.2进入方式	36
6.11.3操作步骤	36
6.11.4相关操作	37
6.11.5异常处理	37
6.11.6输入数据	37
6.11.7输出数据	37
6.11.8操作举例	37
6.12. 查看入侵行为源和目的地址分布报告	38
6.12.1描述	38
6.12.2进入方式	38
6.12.3操作步骤	38
6.12.4相关操作	39
6.12.5异常处理	39
6.12.6输入数据	39
6.12.6输出数据	39
6.12.7操作举例	39
6.13. 查看入侵行为源地址分布报告	40
6.13.1描述	40
6.13.2进入方式	40
6.13.3操作步骤	40
6.13.4相关操作	41
6.13.5异常处理	41
6.13.6输入数据	41
6.13.7输出数据	41
6.13.8操作举例	41
6.14. 查看入侵行为目的地址分布报告	42

6.14.1描述.....	42
6.14.2进入方式.....	42
6.14.3操作步骤.....	42
6.14.4相关操作.....	43
6.14.5异常处理.....	43
6.14.6输入数据.....	43
6.14.7输出数据.....	43
6.14.8操作举例.....	43
6.15. 查询流量信息.....	44
6.15.1描述.....	44
6.15.2进入方式.....	44
6.15.3操作步骤.....	44
6.15.4相关操作.....	45
6.15.5异常处理.....	45
6.15.6输入数据.....	45
6.15.7输出数据.....	46
6.15.8操作举例.....	46
6.16. 查看协议流量分布报告.....	47
6.16.1描述.....	47
6.16.2进入方式.....	47
6.16.3操作步骤.....	47
6.16.4相关操作.....	48
6.16.5异常处理.....	48
6.16.6输入数据.....	48
6.16.7输出数据.....	49
6.16.8操作举例.....	49
6.17. 查看流量变化趋势报告.....	49
6.17.1描述.....	49
6.17.2进入方式.....	50
6.17.3操作步骤.....	50
6.17.4相关操作.....	50
6.17.5异常处理.....	50
6.17.6输入数据.....	50
6.17.7输出数据.....	51
6.17.8操作举例.....	51
6.18. 查看流量 TOP3 报告.....	51

6.18.1描述	51
6.18.2进入方式	51
6.18.3操作步骤	52
6.18.4相关操作	52
6.18.5异常处理	52
6.18.6输入数据	52
6.18.7输出数据	52
6.18.8操作举例	53
6.19. 查看探针安装版本分布报告	53
6.19.1描述	53
6.19.2进入方式	53
6.19.3操作步骤	54
6.19.4相关操作	54
6.19.5异常处理	54
6.19.6输入数据	54
6.19.7输出数据	54
6.19.8操作举例	54
6.20. 查看探针安装趋势报告	55
6.20.1描述	55
6.20.2进入方式	55
6.20.3操作步骤	55
6.20.4相关操作	56
6.20.5异常处理	56
6.20.6输入数据	56
6.20.7输出数据	56
6.20.8操作举例	56
6.21. 查看未安装探针设备报告	57
6.21.1描述	57
6.21.2进入方式	57
6.21.3操作步骤	57
6.21.4相关操作	57
6.21.5异常处理	57
6.21.6输入数据	58
6.21.7输出数据	58
6.21.8操作举例	58
6.22. 查看非最新版本探针报告	58

6.22.1描述	58
6.22.2进入方式	59
6.22.3操作步骤	59
6.22.4相关操作	59
6.22.5异常处理	59
6.22.6输入数据	59
6.22.7输出数据	59
6.22.8操作举例	59
6.23. 查询探针信息	60
6.23.1描述	60
6.23.2进入方式	60
6.23.3操作步骤	60
6.23.4相关操作	60
6.23.5异常处理	61
6.23.6输入数据	61
6.23.7输出数据	61
6.23.8操作举例	61
6.24. 查询设备信息	62
6.24.1描述	62
6.24.2进入方式	62
6.24.3操作步骤	62
6.24.4相关操作	62
6.24.5异常处理	63
6.24.6输入数据	63
6.24.7输出数据	63
6.24.1操作举例	63
6.25. 查询配置信息	64
6.25.1描述	64
6.25.2进入方式	64
6.25.3操作步骤	64
6.25.4相关操作	64
6.25.5异常处理	65
6.25.6输入数据	65
6.25.7输出数据	65
6.25.8操作举例	66
6.26. IP 地址变更查询	66

6.26.1描述.....	66
6.26.2进入方式.....	66
6.26.3操作步骤.....	66
6.26.4相关操作.....	67
6.26.5异常处理.....	67
6.26.6输入数据.....	67
6.26.7输出数据.....	67
6.26.8操作举例.....	67
6.27. 查看 IP 地址变更频度报告	68
6.27.1描述.....	68
6.27.2进入方式.....	68
6.27.3操作步骤.....	68
6.27.4相关操作.....	68
6.27.5异常处理.....	69
6.27.6输入数据.....	69
6.27.7输出数据.....	69
6.27.8操作举例.....	69
6.28. 查看 IP 地址变更趋势报告	70
6.28.1描述.....	70
6.28.2进入方式.....	70
6.28.3操作步骤.....	70
6.28.4相关操作.....	71
6.28.5异常处理.....	71
6.28.6输入数据.....	71
6.28.7输出数据.....	71
6.28.8操作举例.....	71
6.29. 修改密码.....	72
6.29.1描述.....	72
6.29.2进入方式.....	72
6.29.3操作步骤.....	72
6.29.4相关操作.....	72
6.29.5异常处理.....	73
6.29.6输入数据.....	73
6.29.7输出数据.....	73
6.29.8操作举例.....	73
6.30. 网络流量监视.....	73

6.30.1描述	73
6.30.2进入方式	74
6.30.3操作步骤	74
6.30.4相关操作	74
6.30.5异常处理	74
6.30.6输入数据	74
6.30.7输出数据	74
6.30.8操作举例	74
6.31. 安全事件数量监视	75
6.31.1描述	75
6.31.2进入方式	75
6.31.3操作步骤	75
6.31.4相关操作	75
6.31.5异常处理	75
6.31.6输入数据	76
6.31.7输出数据	76
6.31.8操作举例	76
6.32. 查看终端消息	76
6.32.1描述	76
6.32.2进入方式	76
6.32.3操作步骤	77
6.32.4相关操作	77
6.32.5异常处理	77
6.32.6输入数据	77
6.32.7输出数据	77
6.32.8操作举例	77
6.33. 查询日志信息	78
6.33.1描述	78
6.33.2进入方式	78
6.33.3操作步骤	78
6.33.4相关操作	78
6.33.5异常处理	79
6.33.6输入数据	79
6.33.7输出数据	79
6.33.8操作举例	79
6.34. 软件更新	80

6.34.1描述.....	80
6.34.2进入方式.....	80
6.34.3操作步骤.....	80
6.34.4相关操作.....	80
6.34.5异常处理.....	81
6.34.6输入数据.....	81
6.34.7输出数据.....	81
6.34.8操作举例.....	81

1 文档介绍

1.1. 文档目的

睿视行为安全分析和防御系统（以下简称 Insight）使用全面的知识库分析桌面探针行为，提供及时的报警及响应机制。编写本文档是为了指导 Insight 系统的安装、维护和使用。

1.2. 文档范围

本文档描述了 Insight 系统的安装、维护和使用。

缩写，术语	解释
Insight	睿视行为安全分析和防御系统
IDS	Intrusion Detection System 入侵检测系统
Snort	IDS 的一种，是开源和跨平台的 IDS 工具
入侵检测	入侵检测，就是通过从计算机网络或计算机系统若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到袭击的迹象，并对此做出适当反应的过程
桌面探针	具有入侵检测及阻断功能的以协同工作方式的系统称桌面探针
行为	基于 snort 行为规则在网络中抓获的可疑报文而产生的行为
超行为	基于知识库，Insight 对 IDS 行为进行前后件值扩展后的行为；
安全事件	由 Insight 通过知识库对超行为进行相关性分析后，产生的相关行为集合
安全事件图	由安全事件经过 Insight-GAS 和 GUI 分析后展现的图形
知识	对一个行为所需必要条件与行为所造成的后果的简要描述，称为该行为的知识。可供相关性分析算法产生入侵的场景图。
知识库	知识的集合称为知识库

表格 0-1. 术语与缩写解释

2. 系统概述

Insight 是入侵行为安全分析和防御系统，它通过桌面探针实时监控各种数据报文及网络行为，使用知识库对探针行为的相关性提供互动式的分析，帮助安全管理人员从更高的角度来理解攻击的策略，用户使用 Insight 界面控制功能对分析结果进行决策及响应。

3. 运行环境

3.1. 硬件

序号	分项	硬件配置	操作系统
1	数据库服务器	CPU P4 以上, 主频 1.6GHz 以上, 内存 1G 及以上, 硬盘 120G 及以上	Windows Server 2003
2	后台服务器	Intel Xeon(TM) CPU3.0GHz 以上(2 CPUs), 内存 2G 及以上, 硬盘 120G 及以上	Windows Server 2003
3	管理端	CPU P3 以上, 主频 1.6GHz 以上, 内存 1G 及以上, 硬盘 120G 及以上	Windows XP SP2

表格 3-1. 硬件平台配置

3.2. 软件

序号	资源	版本	描述
1	SQLServer 2005i	SP3	用于数据库服务器
2	Microsoft .NET Framework	2.0	用于管理端和服务端

表格 3-2. 软件平台配置

3.3. 网络

序号	资源	配置	描述
1	通信网络	10M/100M 以太网	

表格 3-3. 网络配置

4. 安装

请参考《Insight2.0 环境搭建说明》

5. 启动

图 5-1. 手工启动 Insight 服务端

5.1. 管理端的启动

Insight 管理端通过程序组菜单手工启动。如下图所示：

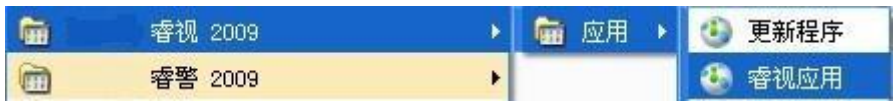


图 5-2. 手工启动 Insight 管理端

6. Insight 管理端使用说明

6.1. 操作界面概述

主界面如下图所示：



图 7-1 管理端主界面

管理端主界面主要由上图中所标的 A、B、C、D、E 五部分组成，他们分别是：

A：菜单栏，点击各个菜单项即可进入相应的操作界面；

B：工具栏，点击工具栏按钮进入各个子系统中常用操作；

C：功能导航区，与菜单栏的功能类似，点击各个项可进入相应的操作界面；

D：工作区，各项操作的界面在该区域显示，以标签页的形式显示；

E：状态栏，显示软件的状态信息和各项操作的结果。

大部分操作界面都显示在工作区中，他们的功能区域布局基本一致，下面以“查询安全事件”界面为例进行说明。下图所示为“查询安全事件”的界面，和大多数操作界面一样，这个界面分为上下两部分，上面部分为“数据输入区”，用于输入数据（如查询条件）、点击按钮操作；下面部分为“数据输出区”，用于展示操作结果数据（如查询结果），在有些情况下可以通过右键菜单对这些数据进行进一步的操作。

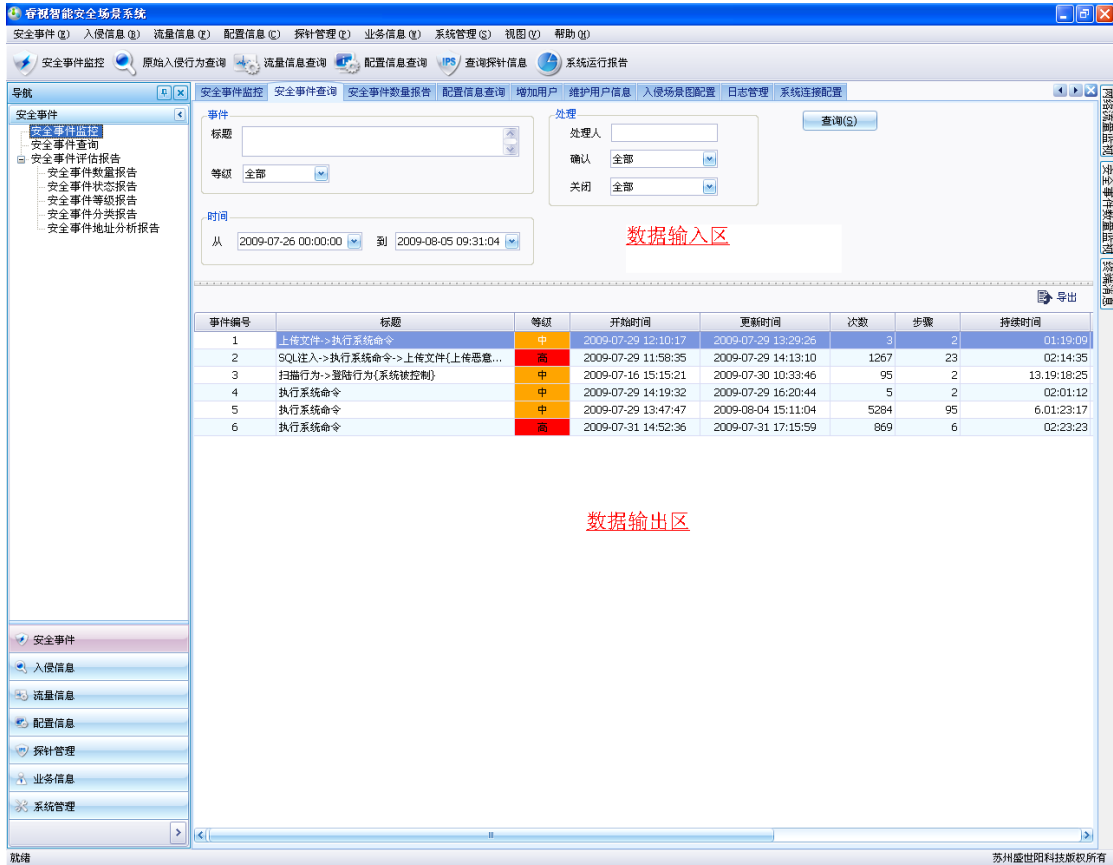


图 7-2 典型操作界面—查询安全事件

6.2. 用户登录

管理端启动后的第一操作界面是用户登录界面，如下图所示：



图 7-3 用户登录界面

6.2.1 操作步骤

- 1、输入账号和密码；
- 2、按“Enter”键或鼠标点击“确定”按钮；
- 3、如果输入的用户名和密码是正确的，则登录成功，进入管理端主界面。

6.2.2 异常处理

如果输入的用户名或密码错误，则登录失败，可进行如下操作之一：

- 1、可以再次输入用户名和密码，重复登录操作；
- 2、按“Esc”键或鼠标点击“取消”按钮退出。

6.3. 实时监控安全事件

用户登录成功后，进入管理端主界面（见图 7-3），主界面中的初始工作界面是“安全事件监控”。

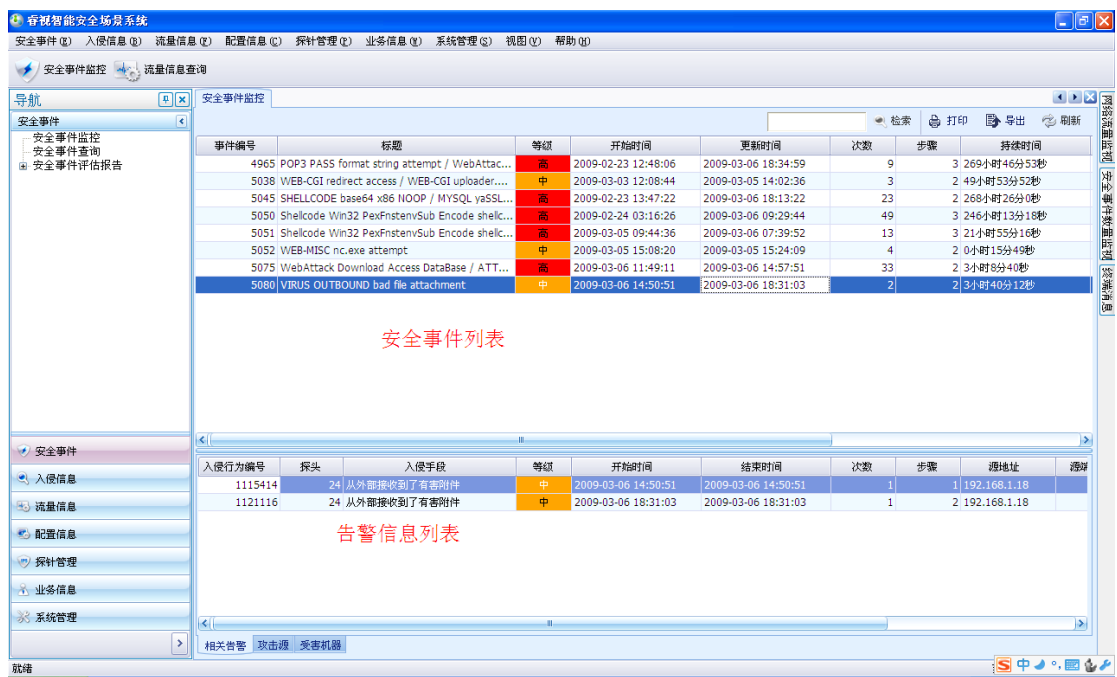


图 7-4 主界面

安全事件监控界面由两部分构成：上面的是“安全事件列表”，其中显示的是未关闭的安全事件（能够实时显示新产生的安全事件）；下面的是“行为信息列表”，其中显示的是“安全事件列表”中被选中的安全事件的行为信息。在“安全事件列表”和“行为信息列表”中可以通过右键菜单进行查看操作。

6.3.1 设置安全事件等级

设置安全事件的等级

1.1.2.1 操作步骤

- 1、选中“安全事件列表”中的某条安全事件，鼠标右键菜单选择“设置安全事件等级”
设置安全事件等级为高、中、低；

1.1.2.2 异常处理

无

6.3.2 安全事件邮件转发

将安全事件以邮件的方式发送给指定的客户

1.1.2.3 操作步骤

- 1、选中“安全事件列表”中的某条安全事件，鼠标右键菜单选择“邮件转发”选择 PDF 格式或者 Excel 格式发送；

1.1.2.4 异常处理

无

6.3.3 查看安全事件

该操作是查看安全事件的详细信息。

1.1.2.5 操作步骤

- 1、选中“安全事件列表”中的某条安全事件，鼠标右键菜单选择“查看安全事件”；
- 2、系统弹出窗口显示该事件的详细信息（见图 7-5）。

安全事件详细信息

基本信息

事件编号

6

标题

执行系统命令

等级

中

开始时间

2009-7-31 14:52:36

次数

869

更新时间

2009-7-31 17:15:59

步骤

6

持续时间

2小时23分23秒

处理情况

☒ 已确认

确认时间

2009-7-31 17:46:11

处理人

处理时间

确定

图 7-5 查看安全事件详细信息界面

1.1.2.6 异常处理

无

6.3.4 确认安全事件

在对安全事件进行查看和分析之后，可以对它进行确认操作。

1.1.2.7 操作步骤

- 1、选中“安全事件列表”中的某条安全事件，鼠标右键菜单选择“确认安全事件”；
- 2、系统在状态栏中反馈操作结果（成功或失败）。

1.1.2.8 异常处理

无

6.3.5 关闭安全事件

在对安全事件进行相关处理和应对后，可以对它进行关闭操作。

1.1.2.9 操作步骤

- 1、选中“安全事件列表”中的某条安全事件，鼠标右键菜单选择“关闭安全事件”；
- 2、系统在状态栏中反馈操作结果（成功或失败）。

1.1.2.10 异常处理

无

6.3.6 关联安全事件

将两个安全事件进行关联。

1.1.2.11 操作步骤

- 1、选中“安全事件列表”中的某条安全事件，鼠标右键菜单选择“关联”；
- 2、系统弹出关联窗口（见图 7-6）。



图 7-6 关联安全事件

3、选择任意一个安全事件，点击关联

1.1.2.12 异常处理

无

6.3.7 查看关联安全事件

查看与某个安全事件关联的所有安全事件

1.1.2.13 操作步骤

- 1、选中“安全事件列表”中的某条安全事件，鼠标右键菜单选择“查看关联安全事件”；
- 2、系统弹出关联窗口（见图 7-7）。



图 7-7 解除关联安全事件

3、选择任意一个安全事件，点击解除关联，可以解除这两个安全事件的关联

1.1.2.14 异常处理

无

6.3.8 查看经验库

查看入侵手段经验库

1.1.2.15 操作步骤

- 1、选中“安全事件列表”中的某条安全事件，鼠标右键菜单选择“查看经验库”；
- 2、系统弹出经验库窗口（见图 7-8）。

查看经验库									
导出									
入侵手段分类	协议	等级	描述	使用工具	预期结果	安全漏洞	安全风险	分析建议	防御建议
发现\Folder_By_hack520 webshell	TCP	高	发现\Folder_By_hack520 webshell, webshell是放在网页服务器上的恶意脚本, 可以用来执行恶意命令的恶意代码。	NULL	NULL	NULL	NULL	1.查找网站的网页是否经过修改, 是否插入eval request恶意语句, 并且恢复文件。2.用相关的工具或脚本进行扫描, 是否安装了木马, 是否有加密的脚本文件, 是否使用了危险的函数, 有的话请删除。3.通过日志分析查看木马如何被上传上来, 并且修补漏洞。	NULL
发现\Folder_By_hack520 webshell	TCP	高	发现\Folder_By_hack520 webshell, webshell是放在网页服务器上的恶意脚本, 可以用来执行恶意命令的恶意代码。	NULL	NULL	NULL	NULL	1.查找网站内网页是否经过修改, 是否插入eval request恶意语句, 并且恢复文件。2.用相关的工具或脚本进行扫描, 是否安装了木马, 是否有加密的脚本文件, 是否使用了危险的函数, 有的话请删除。3.通过日志分析查看木马如何被上传上来, 并且修补漏洞。	NULL
执行TFTP文件传输指令	TCP	中	使用TFTP命令上传或者下载文件	NULL	NULL	NULL	NULL	NULL	NULL
TFTP上传恶意软件	UDP	中	NULL	NULL	NULL	NULL	NULL	NULL	NULL
BACKDOOR 上兴远程控制2008控...	TCP	高	NULL	NULL	NULL	NULL	NULL	NULL	NULL

图 7-8 安全事件经验库

1.1.2.16 异常处理

无

6.3.9 添加处理记录

给安全事件添加处理记录

1.1.2.17 操作步骤

- 1、选中“安全事件列表”中的某条安全事件，鼠标右键菜单选择“添加处理记录”；
- 2、系统弹出添加窗口（见图 7-9）。

图 7-9 添加处理记录

- 3、选择处理类型，设备 IP 地址，补充操作信息，分析结果，获取信息，点击保存；
- 4、点击已有记录，可以查询已经添加的所有处理记录；
- 5、点击关闭，退出添加处理记录。

1.1.2.18 异常处理

无

6.3.10 查看处理记录

查看安全事件的所有处理记录

1.1.2.19 操作步骤

- 1、选中“安全事件列表”中的某条安全事件，鼠标右键菜单选择“查看处理记录”；
- 2、系统弹出处理记录窗口（见图 7-10）。



图 7-10 处理记录

- 3、选择任意一条处理记录，点击删除，可以删除该处理记录；
- 4、对任意一条处理记录修改，点击修改，成功修改；
- 5、点击添加，弹出添加处理记录窗口；

1.1.2.20 异常处理

无

6.3.11 查看攻击手段场景

查看攻击手段场景分布图

1.1.2.21 操作步骤

- 1、选中“安全事件列表”中的某条安全事件，鼠标右键菜单选择“查看攻击手段场景”；
- 2、系统弹出攻击手段场景窗口（见图 7-11）。
- 3、对攻击手段进行相应的处理

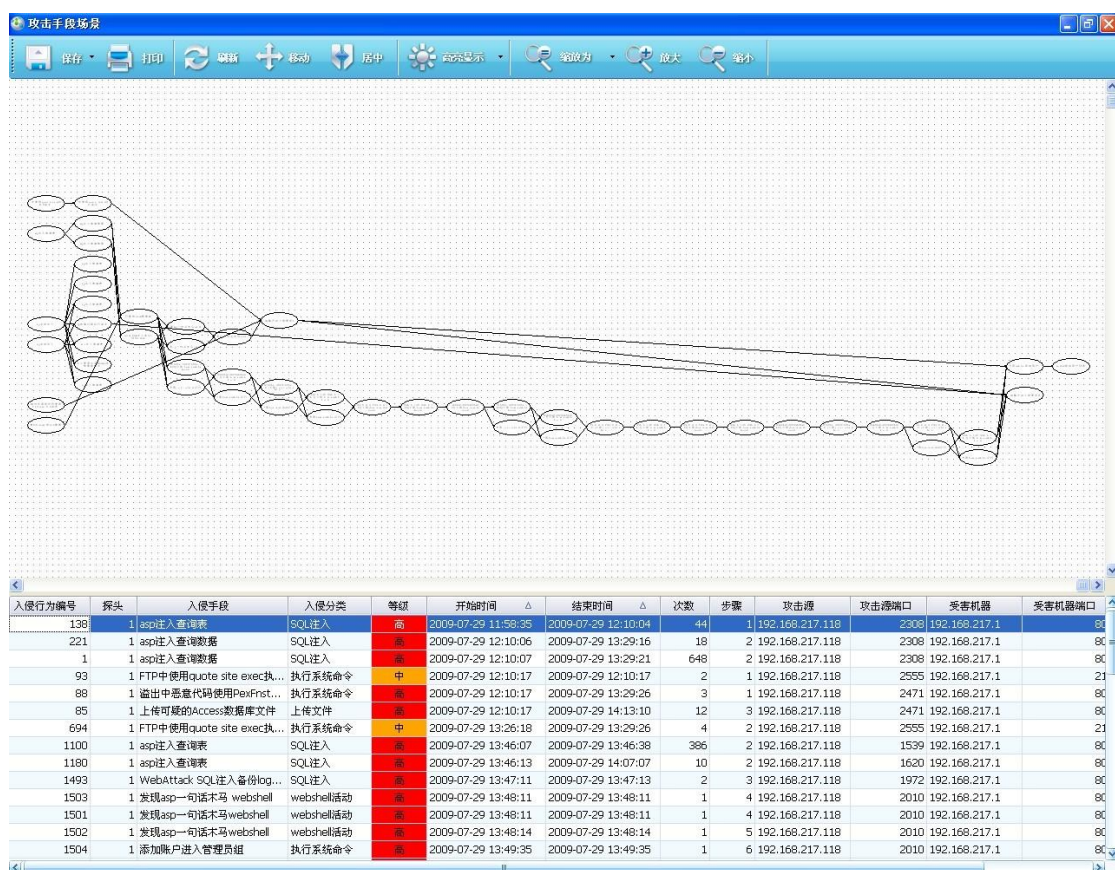


图 7-11 攻击手段场景

1.1.2.22 异常处理

无

6.3.12 查看原始入侵行为

查看某个行为事件的原始入侵行为

1.1.2.23 操作步骤

- 1、选中“行为信息列表”中的一条或多条行为信息，鼠标右键菜单选择“查看原始入侵行为”；
- 2、系统弹出原始入侵行为窗口（见图 7-12）；

[illegible]

6.3.13 发送通知类消息

1.1.2.24 操作步骤

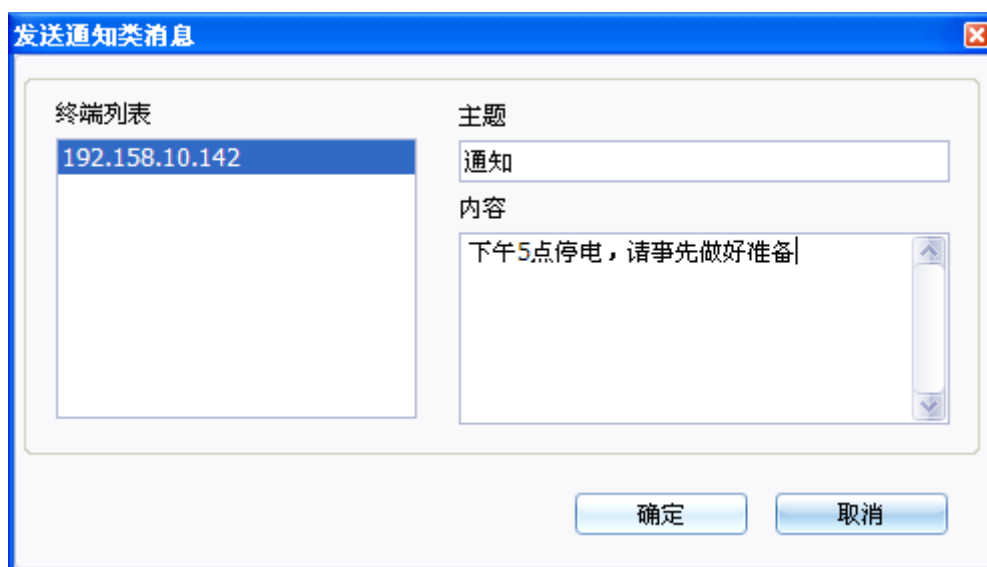


图 7-7 发送通知类消息

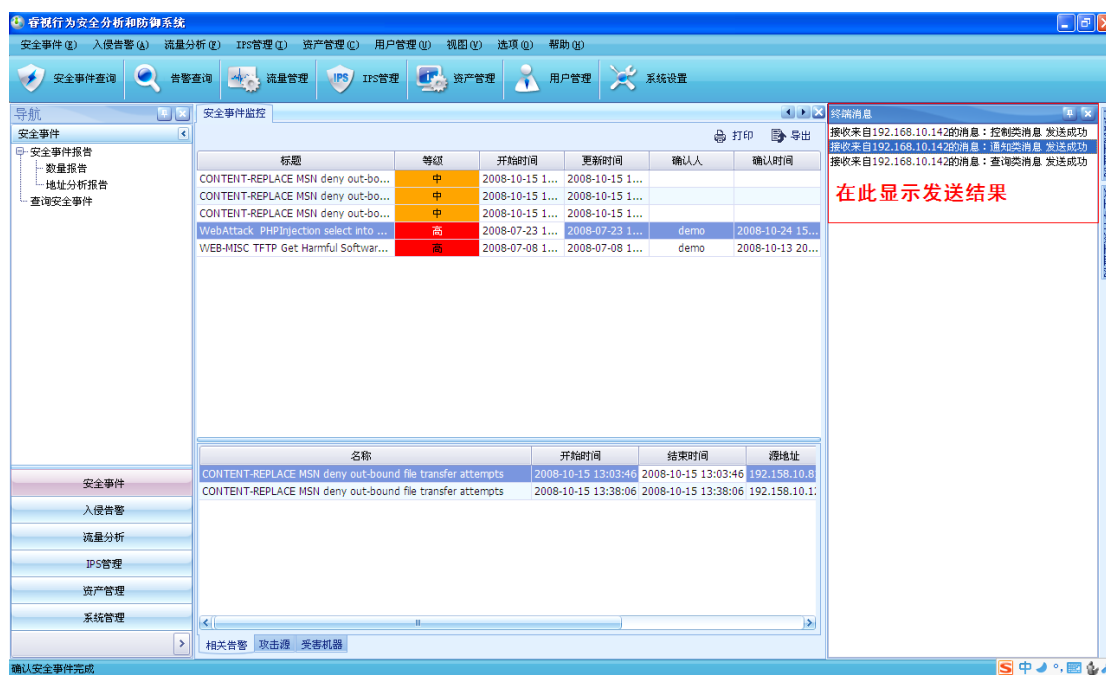


图 7-8 发送结果显示

6.3.14 发送控制类消息

向一个或多个行为信息的目的地址发送控制类消息，让目标机器自动进行某项操作（断网、关机、重启）。

1.1.2.25 操作步骤

- 1、选中“行为信息列表”中的一条或多条行为信息，鼠标右键菜单选择“发送控制类消息”；
- 2、系统弹出对话框进行控制类型的选择和发送操作（见图 7-8）；
- 3、选择控制类型（关机、重启、断网），鼠标点击“确定”按钮；
- 4、系统将控制消息发送到“终端列表”中所显示的 IP 地址（被选中行为信息的目的地址）；
- 5、系统在“终端消息”窗口中显示发送结果（见图 7-7）。

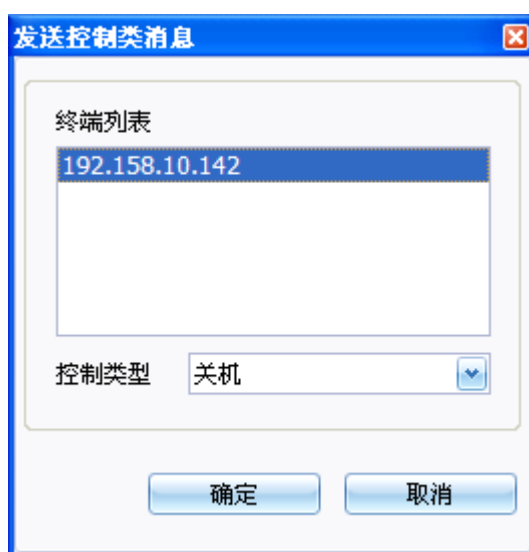


图 7-9 发送控制类消息

1.1.2.26 异常处理

无

6.3.15 查看运行状态

向一个行为信息的目的地址发送查询类消息，实时查看该机器的运行状态、处理器使用率、内存使用量。

1.1.2.27 操作步骤

- 1、选中“行为信息列表”中的一条行为信息，鼠标右键菜单选择“查看运行状态”；
- 2、系统弹出对话框进行发送操作（见图 7-9）；
- 3、鼠标点击“确定”按钮；

- 4、系统将控制消息发送到“终端”中所显示的 IP 地址（被选中行为信息的目的地址）；
- 5、系统在“查询结果”中显示查询结果。

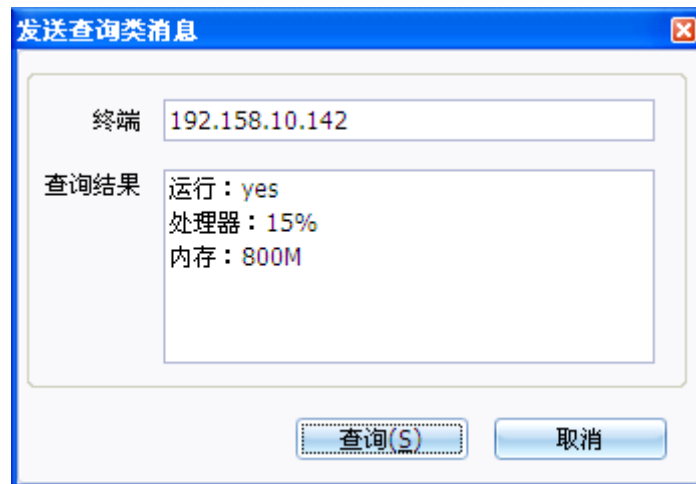


图 7-10 发送查询类消息

1.1.2.28 异常处理

无

6.3.16 查看配置信息

查看行为信息的目的地址所对应的机器的配置（软硬件配置）详细信息。

1.1.2.29 操作步骤

- 1、选中“行为信息列表”中的一条行为信息，鼠标右键菜单选择“查看配置信息”；
- 2、系统弹出对话框显示配置详细信息（见图 7-10）；
- 3、鼠标点击“确定”按钮关闭对话框返回行为信息列表。

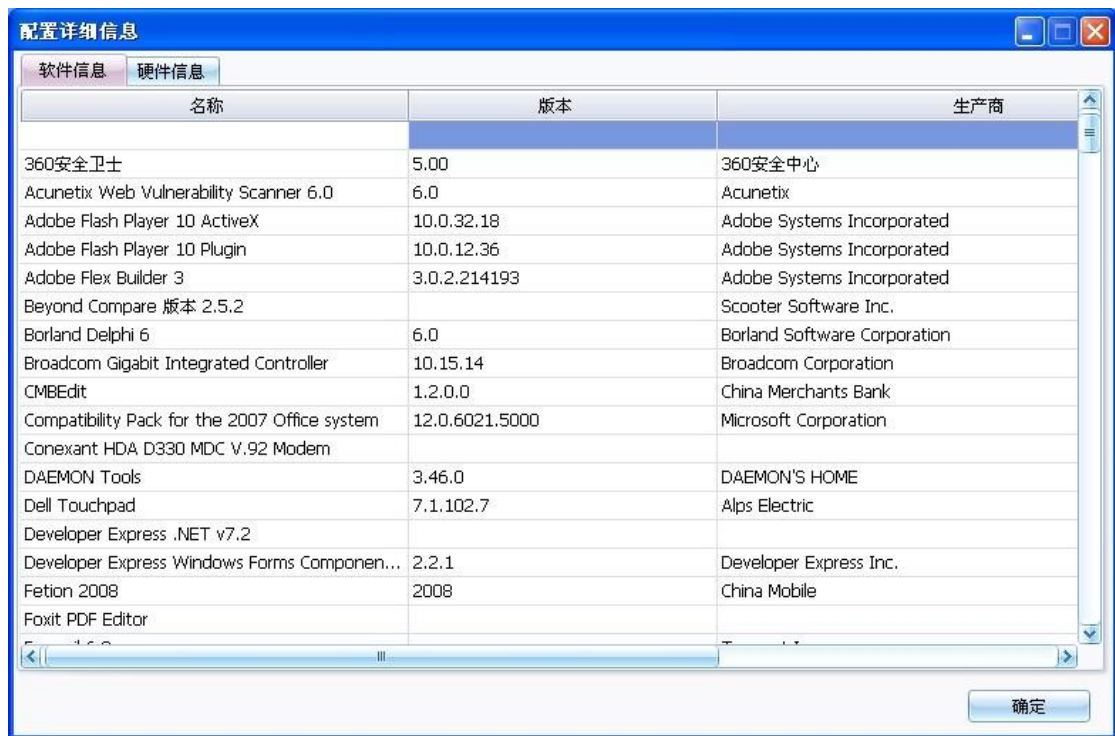


图 7-11 查看配置信息

1.1.2.30 异常处理

无

6.3.17 查看设备信息

查看行为信息的地址所对应的机器的设备信息（所属部门、责任人等）。

1.1.2.31 操作步骤

- 1、选中“行为信息列表”中的一条行为信息，鼠标右键菜单选择“查看设备信息”；
- 2、系统弹出对话框显示设备信息（见图 7-11）；
- 3、鼠标点击“确定”按钮关闭对话框返回行为信息列表。

设备信息			
编号	SSY-YF-200810-0	名称	测试用机
类型	主机	等级	中
所属部门	研发部	责任人	王治国

确定

图 7-12 查看设备信息

1.1.2.32 异常处理

无

6.3.18 查看流量信息

查看行为信息的目的地址从行为开始时间到当前时刻的流量变化趋势(以曲线图的形式展示)。

1.1.2.33 操作步骤

- 1、选中“行为信息列表”中的一条行为信息，鼠标右键菜单选择“查看流量信息”；
- 2、系统弹出对话框显示流量变化曲线图（见图 7-12）；
- 3、鼠标点击“确定”按钮关闭对话框返回行为信息列表。



图 7-13 查看流量信息

1.1.2.34 异常处理

无

6.3.19 查看相关的安全事件

查看行为信息的目的地址相关的安全事件。

1.1.2.35 操作步骤

- 1、选中“行为信息列表”中的一条行为信息，鼠标右键菜单选择“查看安全事件”；
- 2、系统弹出对话框显示与被选中的行为信息的目的地址相关的安全事件(见图 7-13)；
- 3、鼠标点击“确定”按钮关闭对话框返回行为信息列表。

查看安全事件									
导出									
事件编号	标题	等级	开始时间	更新时间	次数	步骤	持续时间	处理人	确认时间
1	SQL注入->执行系统命令->SQ...	高	2009-08-08 13:...	2009-08-08 18:1...	330	4	04:56:40	luquan	2009-08-08 1
3	上传文件->执行系统命令->木...	中	2009-08-08 13:...	2009-08-08 13:4...	27	2	00:22:35	super	2009-08-08 2
4	SQL注入->执行系统命令->扫...	高	2009-08-08 18:...	2009-08-08 20:2...	663	8	01:51:51	super	2009-08-08 2
5	上传文件->执行系统命令->木...	高	2009-08-08 18:...	2009-08-08 20:2...	35	2	02:10:58		2009-08-10 1

图 7-14 查看行为相关的安全事件

1.1.2.36 异常处理

无

6.4. 查询安全事件

6.4.1 描述

输入多个查询条件，根据查询条件检索出符合条件的安全事件，并可对查询结果中的安全事件列表进行进一步的操作（查看原始图、查看聚合图、查看详细信息、确认事件、关闭事件）。

6.4.2 进入方式

- 1、菜单项：“安全事件”->“安全事件查询”；
- 2、导航栏：“安全事件”->“安全事件查询”。

6.4.3 操作步骤

- 1、在查询条件（详见输入数据）中输入要查询的内容（如果某个查询条件不输入内容，表示对该条件不作限制，初始状态下对所有条件不作限制），点击“查询”按钮；
- 2、系统以安全事件列表的形式给出查询结果。

6.4.4 相关操作

对于查询结果，可以通过右键菜单进行如下操作：

- 1、查看安全事件，详见 7.3.3；
- 2、邮件转发，详见 7.3.2；
- 3、查看关联事件，详见 7.3.7；
- 4、查看经验库，详见 7.3.8；
- 4、查看处理记录，详见 7.3.101；
- 5、查看攻击手段场景，详见 7.3.11。

6.4.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；

2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.4.6 输入数据

名称	说明	输入举例
标题	安全事件的标题	CONTENT-REPLACE MSN deny out-bound file transfer attempts
等级	安全事件的等级，如选择 ALL 表示对该条件不作限制	高
开始时间或更新时间范围	安全事件的开始时间或更新时间的范围（在设定范围内的安全事件符合查询条件）	从 2008-10-18 到 2008-10-26
处理人	关闭或确认安全事件的人员	Admin
确认	安全事件是否确认，如选择 ALL 表示对该条件不作限制	是
关闭	安全事件是否关闭，如选择 ALL 表示对该条件不作限制	否

表格 6-1 安全事件查询输入数据表

6.4.7 输出数据

名称	说明	输出举例
标题	安全事件的标题	CONTENT-REPLACE MSN deny out-bound file transfer attempts
等级	安全事件的等级	高
开始时间	安全事件的开始时间	2008-7-10 16:44:19
更新时间	安全事件被更新的时间	2008-7-10 17:02:13
处理人	关闭或确认安全事件的人员	Admin
确认时间	安全事件被确认的时间	2008-10-10 20:42:28
关闭时间	安全事件被关闭的时间	2008-10-10 21:00:27

表格 6-2 安全事件查询输出数据表

6.4.8 操作举例

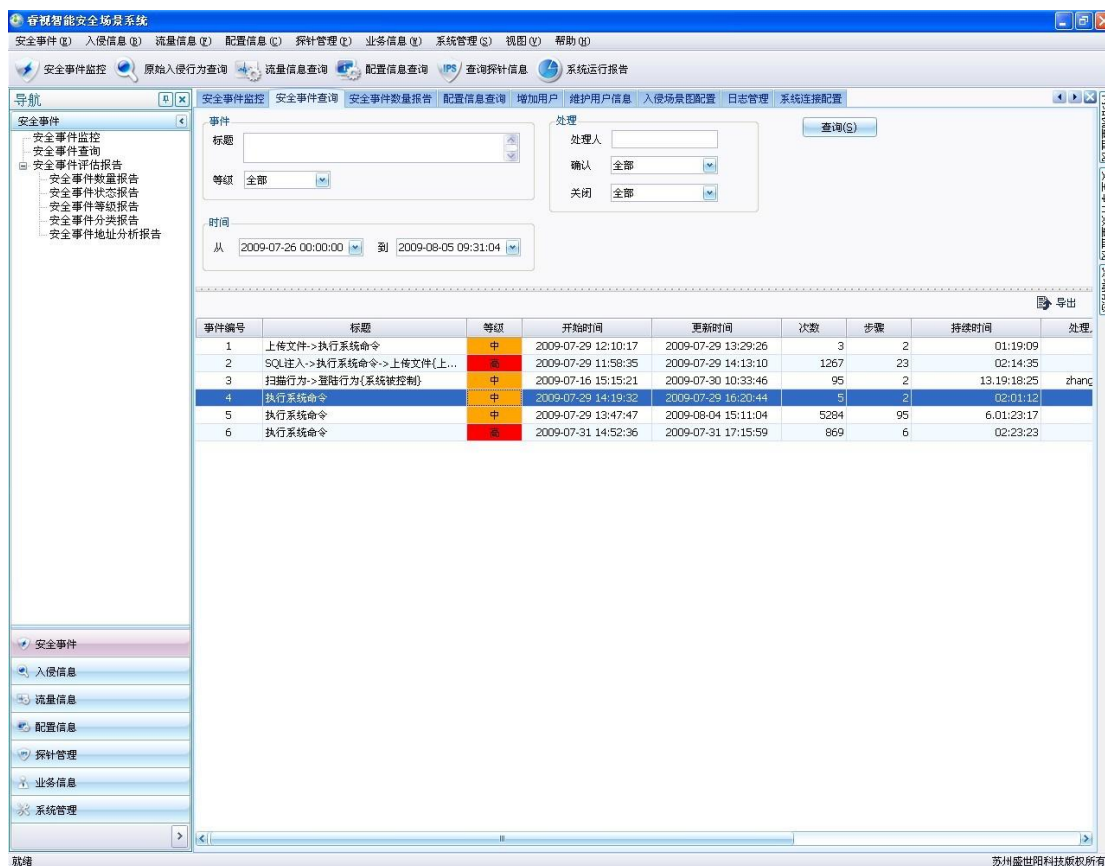


图 7-15 安全事件查询

6.5. 查看安全事件数量报告

6.5.1 描述

查看安全事件数量年报（指定的年中每个月的安全事件数量）、数量月报（指定的月中每一周的安全事件数量）、数量周报（指定的周中每一天的安全事件数量），这些报表都以柱状图的形式展示。

6.5.2 进入方式

- 1、菜单项：“安全事件”->“安全事件评估报告”->“安全事件数量报告”；
- 2、导航栏：“安全事件”->“安全事件评估报告”->“安全事件数量报告”。

6.5.3 操作步骤

- 1、选择报表类型（年报/月报/周报）；

- 2、如果选中了年报，则必须输入具体的年；如果选中了月报，则必须输入具体的年和月；如果选中了周报，则必须输入具体的年、月和周；
- 3、点击“查询”按钮；
- 4、系统以柱状图的形式给出报表。

6.5.4 相关操作

无

6.5.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.5.6 输入数据

名称	说明	输入举例
报表类型	报表的类型：年报、月报、周报	年报
年	某一年的年报或者是某年某月的月报或者是某年某月某周的周报	2008
月	某年某月的月报或者是某年某月某周的周报	7
周	查看周报时的某年某月的第几周	1

表格 6-3 安全事件数量报表输入数据表

6.5.7 输出数据

名称	说明	输出举例
柱状图横坐标	年报时为 1 月—12 月；月报时为第一周—第四周；周报时为该周的星期一—星期日	第一周、第二周、第三周、第四周
柱状图纵坐标	某月/某周/某天的安全事件数量	100

表格 6-4 安全事件数量报表输出数据表

6.5.8 操作举例



图 7-17 安全事件数量报表

6.6. 查看安全事件等级报告

6.6.1 描述

查看安全事件高中低个数和比例，这些报表都以饼状图的形式展示。

6.6.2 进入方式

- 1、菜单项：“安全事件”->“安全事件评估报告”->“安全事件等级报告”；
- 2、导航栏：“安全事件”->“安全事件评估报告”->“安全事件等级报告”。

6.6.3 操作步骤

- 1、选择报表类型（年报/月报/周报）；
- 2、如果选中了年报，则必须输入具体的年；如果选中了月报，则必须输入具体的年和月；如果选中了周报，则必须输入具体的年、月和周；
- 3、点击“查询”按钮；
- 4、系统以饼状图的形式给出报表。

6.6.4 相关操作

无

6.6.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.6.6 输入数据

名称	说明	输入举例
报表类型	报表的类型：年报、月报、周报	年报
年	某一年的年报或者是某年某月的月报或者是某年某月某周的周报	2009
月	某年某月的月报或者是某年某月某周的周报	7
周	查看周报时的某年某月的第几周	5

表格 6-5 安全事件等级报表输入数据表

6.6.7 输出数据

名称	说明	输出举例
安全事件等级报告	高中低安全事件的比例	高等级安全事件百分数、中等级安全事件百分数、低等级安全事件百分数

表格 6-6 安全事件等级报表输出数据表

6.6.8 操作举例

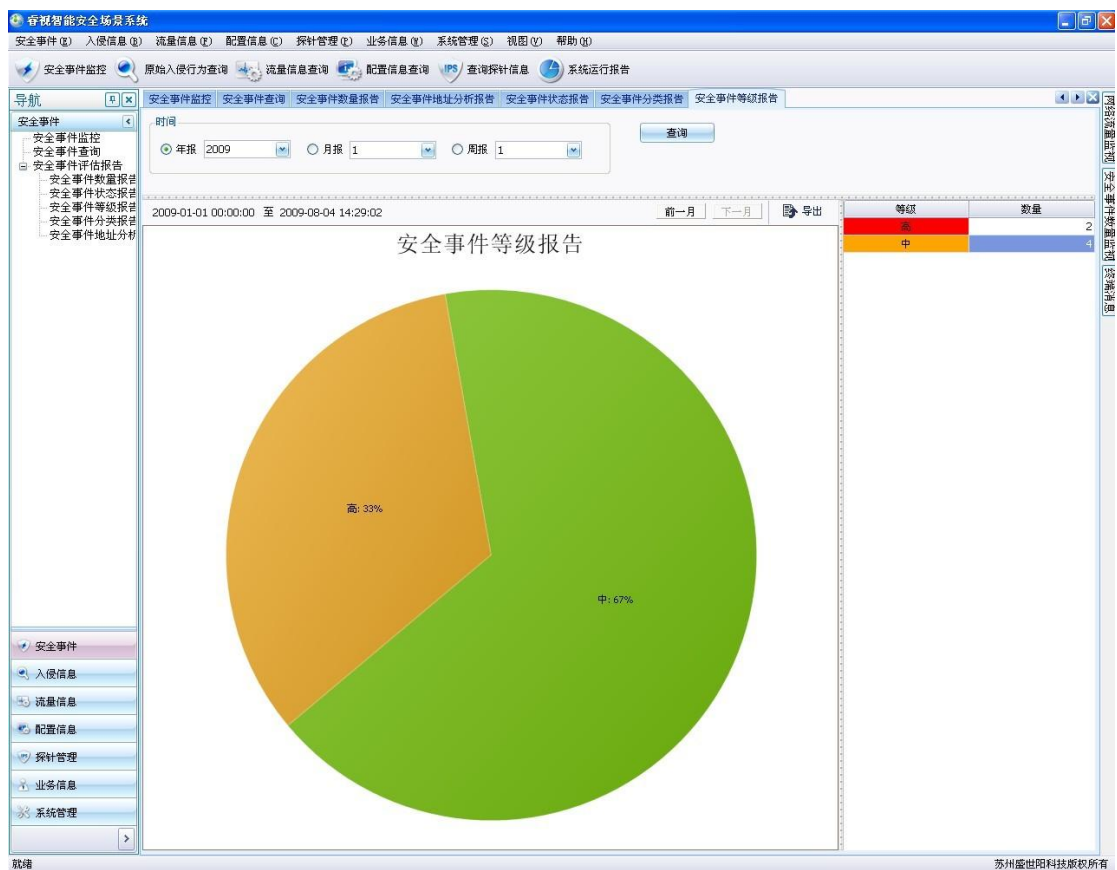


图 7-17 安全事件等级报表

6.7. 查看安全事件状态报告

6.7.1 描述

查看安全事件状态年报（指定的年中各个状态的安全事件数量）、状态月报（指定的月中各个状态的安全事件数量）、状态周报（指定的周中各个状态的安全事件数量），这些报表都以柱状图的形式展示。

6.7.2 进入方式

- 1、菜单项：“安全事件”->“安全事件评估报告”->“安全事件状态分析报告”；
- 2、导航栏：“安全事件”->“安全事件评估报告”->“安全事件状态分析报告”。

6.7.3 操作步骤

- 1、选择报表类型（年报/月报/周报）；

- 2、如果选中了年报，则必须输入具体的年；如果选中了月报，则必须输入具体的年和月；如果选中了周报，则必须输入具体的年、月和周；
- 3、点击“查询”按钮；
- 4、系统以柱状图的形式给出报表。

6.7.4 相关操作

无

6.7.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.7.6 输入数据

名称	说明	输入举例
报表类型	报表的类型：年报、月报、周报	年报
年	某一年的年报或者是某年某月的月报或者是某年某月某周的周报	2008
月	某年某月的月报或者是某年某月某周的周报	7
周	查看周报时的某年某月的第几周	1

表格 6-7 安全事件状态分析报表输入数据表

6.7.7 输出数据

名称	说明	输出举例
柱状图横坐标	安全事件的状态（未确认未关闭、已确认、已关闭）	未确认未关闭、已确认、已关闭
柱状图纵坐标	某个状态的安全事件数量	100

表格 6-8 安全事件状态分析报表输出数据表

6.7.8 操作举例



图 7-19 安全事件状态分析报表

6.8. 查询入侵行为

6.8.1 描述

输入多个查询条件，根据查询条件检索出符合条件的入侵行为，并可对查询结果中的入侵行为列表进行进一步的操作（发送通知类消息、发送控制类消息、发送查询类消息、查看配置信息、查看设备信息、查看流量信息、查看相关的安全事件）。

6.8.2 进入方式

- 1、菜单项：“入侵信息”->“原始入侵行为查询”；
- 2、导航栏：“入侵信息”->“原始入侵行为查询”。

6.8.3 操作步骤

- 1、在查询条件（详见输入数据）中输入要查询的内容（如果某个查询条件不输入内容，表示对该条件不作限制，初始状态下对所有条件不作限制），点击“查询”按钮；
- 2、系统以入侵行为信息列表的形式给出查询结果。

6.8.4 相关操作

对于查询结果，可以通过右键菜单进行如下操作：

1. 发送通知类消息，详见 7.3.13;
2. 发送控制类消息，详见 7.3.14;
3. 查看运行状态，详见 7.3.16;
4. 查看配置信息，详见 7.3.17;
5. 查看设备信息，详见 7.3.18;
6. 查看流量信息，详见 7.3.19;
7. 查看相关的安全事件，详见 7.3.20。

6.8.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.8.6 输入数据

名称	说明	输入举例
名称	入侵行为的名称	ICMP Echo Reply
等级	入侵行为的等级，如选择 ALL 表示对该条件不作限制	高
协议	与入侵行为相关的网络协议（TCP、UDP、ICMP、ARP）	UDP
探头	产生入侵行为的 IDS 或探针的编号	18
源 IP 地址	攻击源的 IP 地址	192.158.10.142
目的 IP 地址	受害者的 IP 地址	192.158.10.188
时间范围	入侵行为的开始时间和结束时间在设定范围内则符合查询条件	从 2008-10-18 到 2008-10-26

表格 6-9 入侵行为查询输入数据表

6.8.7 输出数据

名称	说明	输出举例
名称	入侵行为的名称	ICMP Echo Reply
开始时间	入侵行为的开始时间	2008-10-13 12:55:27
结束时间	入侵行为的结束时间	2008-10-13 12:55:27
攻击源	攻击源的 IP 地址	192.158.10.142
攻击源端口	攻击源的端口号	6534
受害机器	受害者的 IP 地址	192.158.10.188

受害机器端口	受害者的端口号	80
协议	与入侵行为相关的网络协议（TCP、UDP、ICMP、ARP）	UDP

表格 6-10 入侵行为查询输出数据表

6.8.8 操作举例

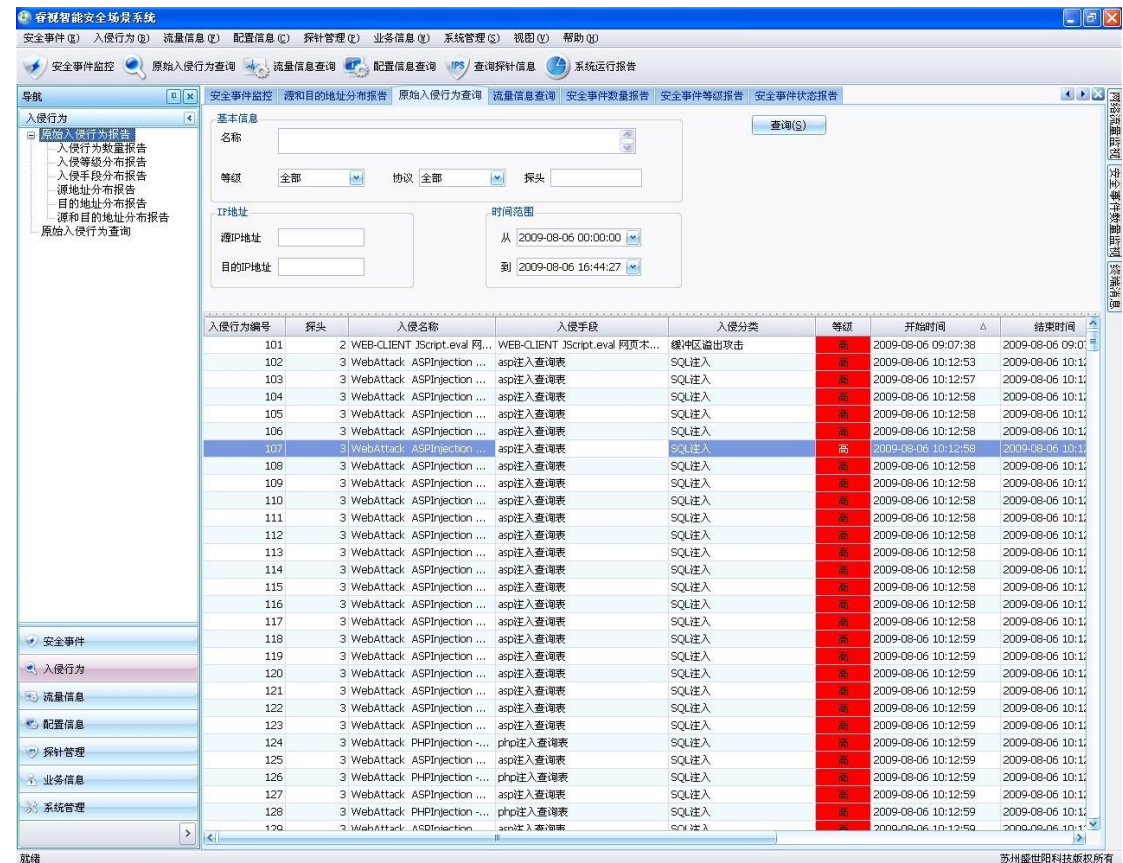


图 7-20 入侵行为查询

6.9. 查看入侵行为数量报告

6.9.1 描述

查看入侵行为数量年报（指定的年中每个月的入侵行为数量）、数量月报（指定的月中每一周的入侵行为数量）、数量周报（指定的周中每一天的入侵行为数量），这些报表都以柱状图的形式展示。

6.9.2 进入方式

- 1、菜单项：“入侵信息”->“原始入侵行为报告”->“入侵行为数量报告”；
- 2、导航栏：“入侵信息”->“原始入侵行为报告”->“入侵行为数量报告”。

6.9.3 操作步骤

- 1、选择报表类型（年报/月报/周报）；
- 2、如果选中了年报，则必须输入具体的年；如果选中了月报，则必须输入具体的年和月；如果选中了周报，则必须输入具体的年、月和周；
- 3、点击“查询”按钮；
- 4、系统以柱状图的形式给出报表。

6.9.4 相关操作

无

6.9.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.9.6 输入数据

名称	说明	输入举例
报表类型	报表的类型：年报、月报、周报	年报
年	某一年的年报或者是某年某月的月报或者是某年某月某周的周报	2008
月	某年某月的月报或者是某年某月某周的周报	7
周	查看周报时的某年某月的第几周	1

表格 6-11 入侵行为数量报表输入数据表

6.9.7 输出数据

名称	说明	输出举例
柱状图横坐标	年报时为 1 月—12 月；月报时为第一周—第四周；周报时为该周的星期一—星期日	第一周、第二周、第三周、第四周
柱状图纵坐标	某月/某周/某天的入侵行为数量	100

表格 6-12 入侵行为数量报表输出数据表

6.9.8 操作举例



图 7-21 入侵行为数量报表

6.10. 查看入侵行为等级分析报告

6.10.1 描述

查看入侵行为等级分析年报（指定的年中各类等级的入侵行为的数量和比例）、等级分析月报（指定的月中各类等级的入侵行为的数量和比例）、等级分析周报（指定的周中各类等级的入侵行为的数量和比例），以列表的形式给出给类等级的行为数量，以饼图的形式给出各类等级行为的比例。

6.10.2 进入方式

- 1、菜单项：“入侵信息”->“原始入侵行为报告”->“入侵等级分布报告”；
- 2、导航栏：“入侵信息”->“原始入侵行为报告”->“入侵等级分布报告”。

6.10.3 操作步骤

- 1、选择报表类型（年报/月报/周报）；
- 2、如果选中了年报，则必须输入具体的年；如果选中了月报，则必须输入具体的年和月；如果选中了周报，则必须输入具体的年、月和周；
- 3、点击“查询”按钮；

4、系统以饼图和列表的形式给出报表。

6.10.4 相关操作

无

6.10.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.10.6 输入数据

名称	说明	输入举例
报表类型	报表的类型：年报、月报、周报	年报
年	某一年的年报或者是某年某月的月报或者是某年某月某周的周报	2009
月	某年某月的月报或者是某年某月某周的周报	7
周	查看周报时的某年某月的第几周	1

表格 6-13 入侵行为等级分析报表输入数据表

6.10.7 输出数据

名称	说明	输出举例
等级	入侵行为的等级（高、中、低）	高
数量	某等级的入侵行为的数量	100

表格 6-14 入侵行为等级分析报表输出数据表

6.10.8 操作举例

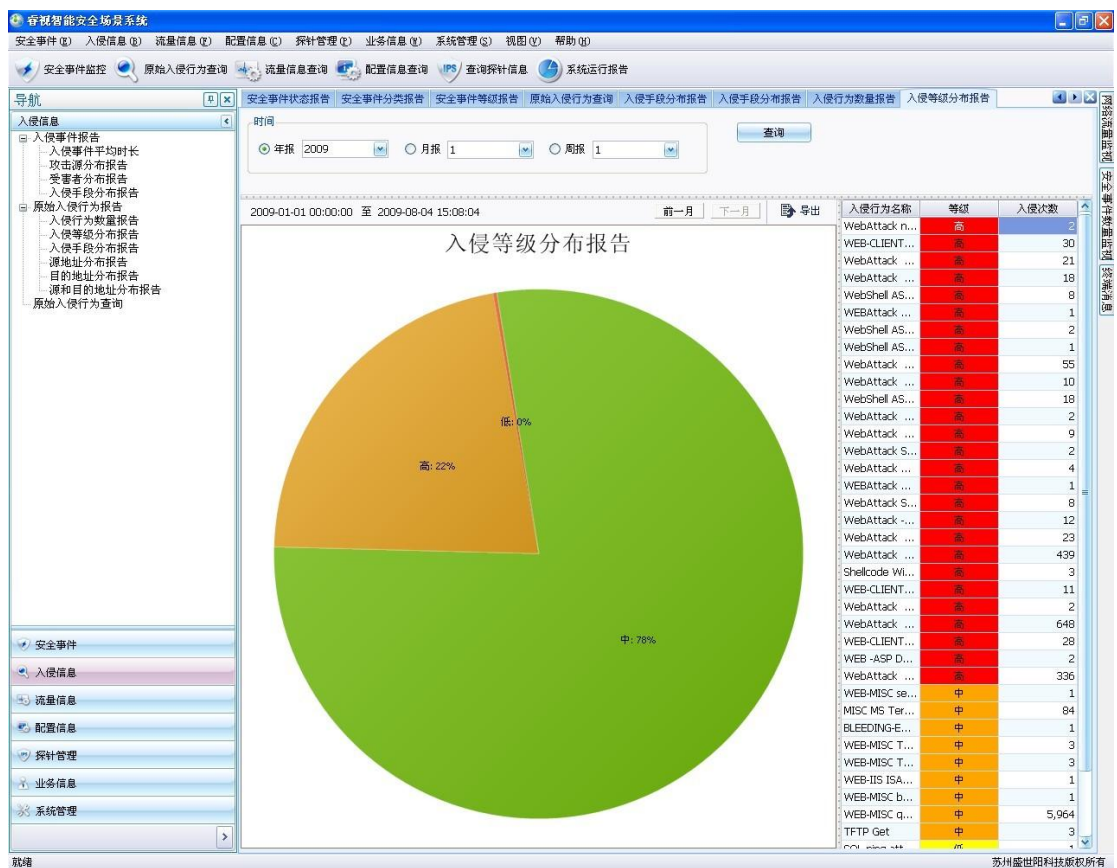


图 7-22 入侵行为等级分析报表

6.11. 查看入侵手段分布报告

6.11.1 描述

查看入侵方法统计年报（指定的年中各种类的入侵行为的数量和比例）、种类统计月报（指定的月中各种类的入侵行为的数量和比例）、种类统计周报（指定的周中各种类的入侵行为的数量和比例），以列表的形式给出给种类的行为数量，以饼图的形式给出各种类行为的比例（只列出比例前三名，三名之后的被累加为“其他”显示）。

6.11.2 进入方式

- 1、菜单项：“入侵信息”->“原始入侵行为报告”->“入侵手段分布报告”；
- 2、导航栏：“入侵信息”->“原始入侵行为报告”->“入侵手段分布报告”。

6.11.3 操作步骤

- 1、选择报表类型（年报/月报/周报）；

- 2、如果选中了年报，则必须输入具体的年；如果选中了月报，则必须输入具体的年和月；如果选中了周报，则必须输入具体的年、月和周；
- 3、点击“查询”按钮；
- 4、系统以饼图和列表的形式给出报表。

6.11.4 相关操作

无

6.11.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.11.6 输入数据

名称	说明	输入举例
报表类型	报表的类型：年报、月报、周报	年报
年	某一年的年报或者是某年某月的月报或者是某年某月某周的周报	2009
月	某年某月的月报或者是某年某月某周的周报	7
周	查看周报时的某年某月的第几周	1

表格 6-15 入侵方法分布报告输入数据表

6.11.7 输出数据

名称	说明	输出举例
行为类型	入侵行为的种类	MISC UPnP malformed advertisement 30
数量	某种类的入侵行为的数量	30

表格 6-16 入侵手段分布报告输出数据表

6.11.8 操作举例

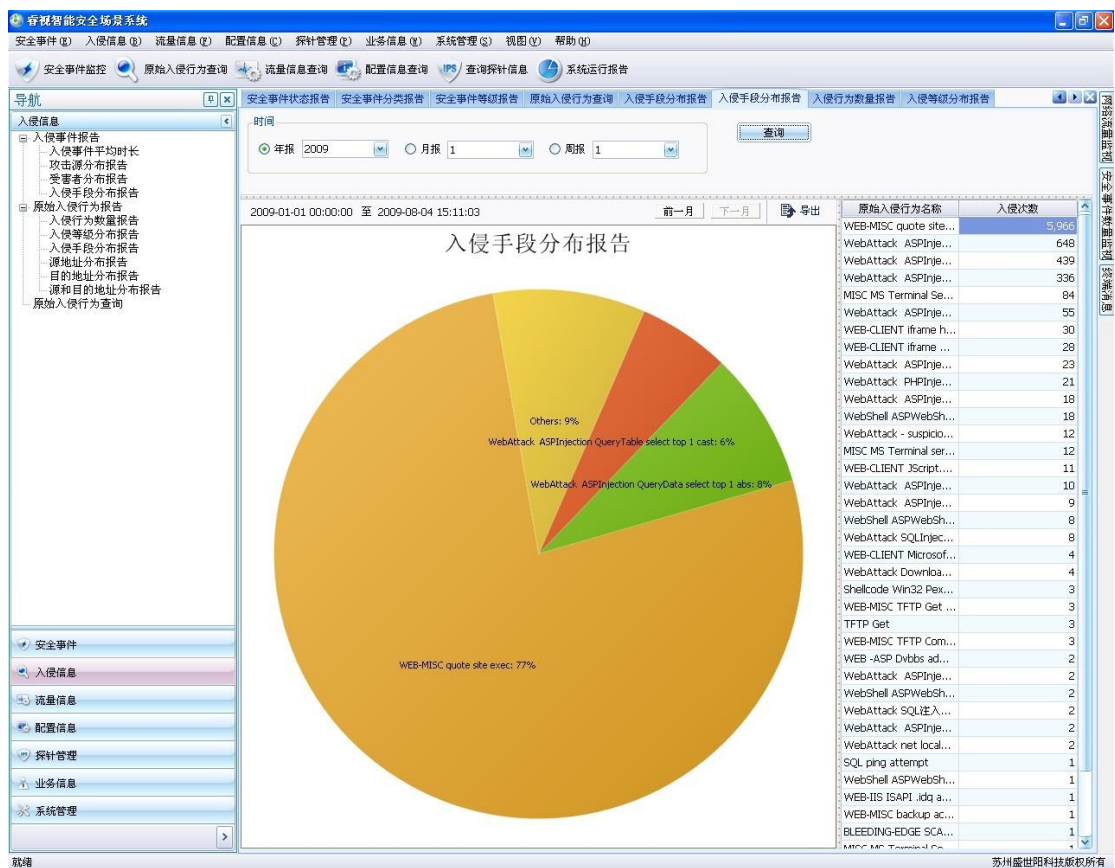


图 7-23 入侵手段分布报告

6.12. 查看入侵行为源和目的地址分布报告

6.12.1 描述

查看入侵行为源和目的地址分布年报(指定的年中相同源和目的地址的入侵行为的数量和比例)、源和目的地址统计月报(指定的月中相同源和目的地址的入侵行为的数量和比例)、源和目的地址统计周报(指定的周中相同源和目的地址的入侵行为的数量和比例)，以列表的形式给出源和目的地址对的行为数量，以饼图的形式给出源和目的地址对的行为的比例（只列出比例前三名，三名之后的被累加为“其他”显示）。

6.12.2 进入方式

- 1、菜单项：“入侵信息”->“原始入侵行为报告”->“源和目的地址分布报告”；
- 2、导航栏：“入侵信息”->“原始入侵行为报告”->“源和目的地址分布报告”。

6.12.3 操作步骤

- 1、选择报表类型（年报/月报/周报）；

- 2、如果选中了年报，则必须输入具体的年；如果选中了月报，则必须输入具体的年和月；如果选中了周报，则必须输入具体的年、月和周；
- 3、点击“查询”按钮；
- 4、系统以饼图和列表的形式给出报表。

6.12.4 相关操作

无

6.12.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.12.6 输入数据

名称	说明	输入举例
报表类型	报表的类型：年报、月报、周报	年报
年	某一年的年报或者是某年某月的月报或者是某年某月某周的周报	2009
月	某年某月的月报或者是某年某月某周的周报	7
周	查看周报时的某年某月的第几周	5

表格 6-17 入侵行为源和目的地址统计报表输入数据表

6.12.6 输出数据

名称	说明	输出举例
源 IP 地址	入侵行为攻击源的 IP 地址	192.158.10.51
目的 IP 地址	入侵行为受害者的 IP 地址	192.158.10.72
行为数量	源 IP 地址和目的 IP 地址所对应的行为数量	5284

表格 6-18 入侵行为源和目的地址统计报表输出数据表

6.12.7 操作举例

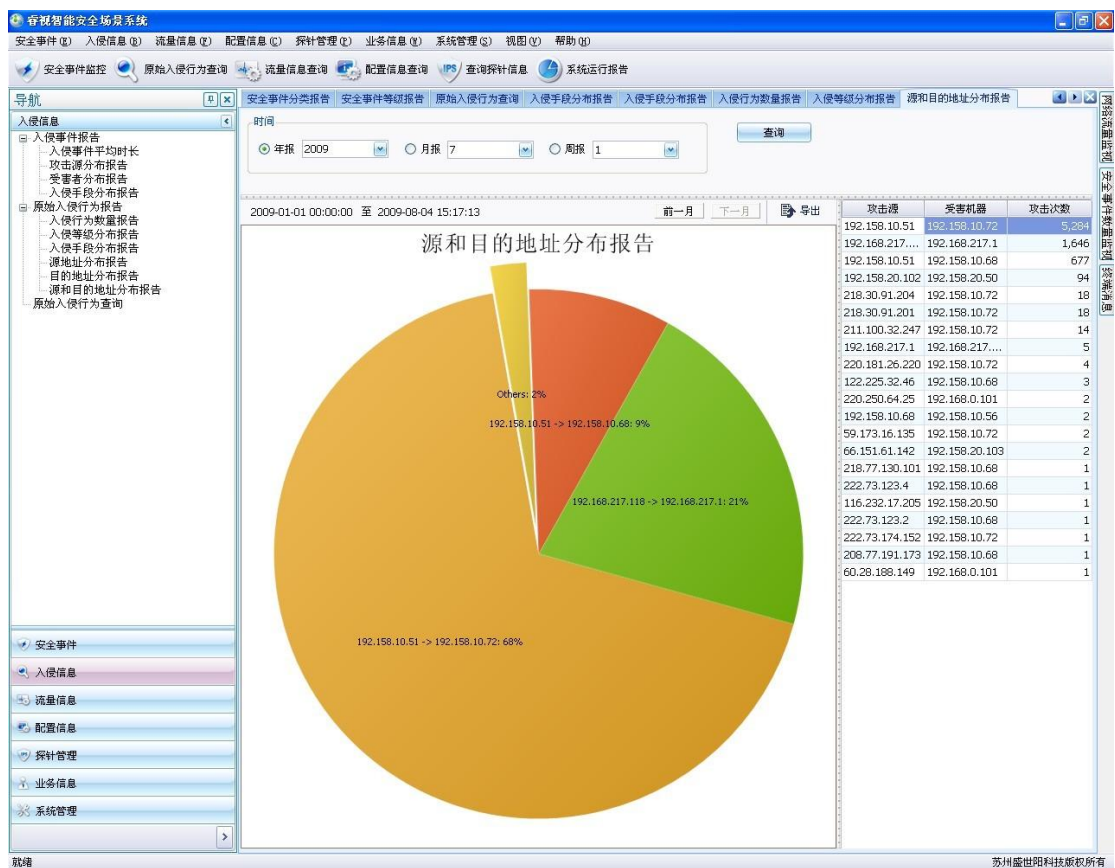


图 7-24 入侵行为源和目的地址统计报表

6.13. 查看入侵行为源地址分布报告

6.13.1 描述

查看入侵行为源地址统计年报（指定的年中相同源地址的入侵行为的数量和比例）、源地址统计月报（指定的月中相同源地址的入侵行为的数量和比例）、源地址统计周报（指定的周中相同源地址的入侵行为的数量和比例），以列表的形式给出各个源地址的行为数量，以饼图的形式给出各个源地址的行为的比例（只列出比例前三名，三名之后的被累加为“其他”显示）。

6.13.2 进入方式

- 1、菜单项：“入侵信息”->“原始入侵行为报告”->“源地址分布报告”；
- 2、导航栏：“入侵信息”->“原始入侵行为报告”->“源地址分布报告”。

6.13.3 操作步骤

- 1、选择报表类型（年报/月报/周报）；

- 2、如果选中了年报，则必须输入具体的年；如果选中了月报，则必须输入具体的年和月；如果选中了周报，则必须输入具体的年、月和周；
- 3、点击“查询”按钮；
- 4、系统以饼图和列表的形式给出报表。

6.13.4 相关操作

无

6.13.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.13.6 输入数据

名称	说明	输入举例
报表类型	报表的类型：年报、月报、周报	年报
年	某一年的年报或者是某年某月的月报或者是某年某月某周的周报	2009
月	某年某月的月报或者是某年某月某周的周报	7
周	查看周报时的某年某月的第几周	1

表格 6-19 入侵行为源地址统计报表输入数据表

6.13.7 输出数据

名称	说明	输出举例
源 IP 地址	入侵行为攻击源的 IP 地址	192. 158. 20. 102
行为数量	源 IP 地址所对应的行为数量	4

表格 6-20 入侵行为源地址统计报表输出数据表

6.13.8 操作举例

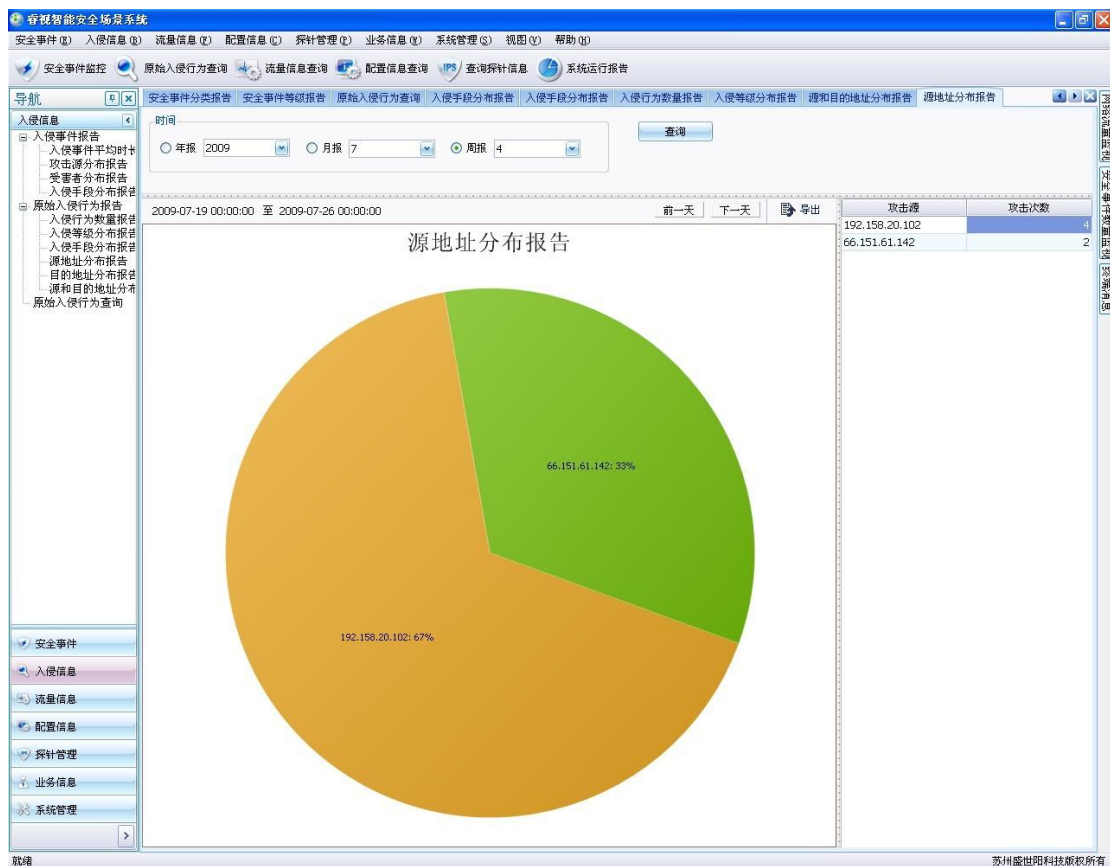


图 7-25 入侵行为源地址统计报表

6.14. 查看入侵行为目的地址分布报告

6.14.1 描述

查看入侵行为目的地址统计年报(指定的年中相同目的地址的入侵行为的数量和比例)、目的地址统计月报(指定的月中相同目的地址的入侵行为的数量和比例)、目的地址统计周报(指定的周中相同目的地址的入侵行为的数量和比例),以列表的形式给出各个目的地址的行为数量,以饼图的形式给出各个目的地址的行为的比例(只列出比例前三名,三名之后的被累加为“其他”显示)。

6.14.2 进入方式

- 1、菜单项:“入侵信息”->“入侵行为报告”->“目的地址分布报告”;
- 2、导航栏:“入侵信息”->“入侵行为报告”->“目的地址分布报告”。

6.14.3 操作步骤

- 1、选择报表类型(年报/月报/周报);

- 2、如果选中了年报，则必须输入具体的年；如果选中了月报，则必须输入具体的年和月；如果选中了周报，则必须输入具体的年、月和周；
- 3、点击“查询”按钮；
- 4、系统以饼图和列表的形式给出报表。

6.14.4 相关操作

无

6.14.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.14.6 输入数据

名称	说明	输入举例
报表类型	报表的类型：年报、月报、周报	年报
年	某一年的年报或者是某年某月的月报或者是某年某月某周的周报	2009
月	某年某月的月报或者是某年某月某周的周报	7
周	查看周报时的某年某月的第几周	1

表格 6-21 入侵行为目的地址统计报表输入数据表

6.14.7 输出数据

名称	说明	输出举例
目的 IP 地址	入侵行为受害者的 IP 地址	192. 158. 10. 72
行为数量	目的 IP 地址所对应的行为数量	3300

表格 6-22 入侵行为目的地址统计报表输出数据表

6.14.8 操作举例

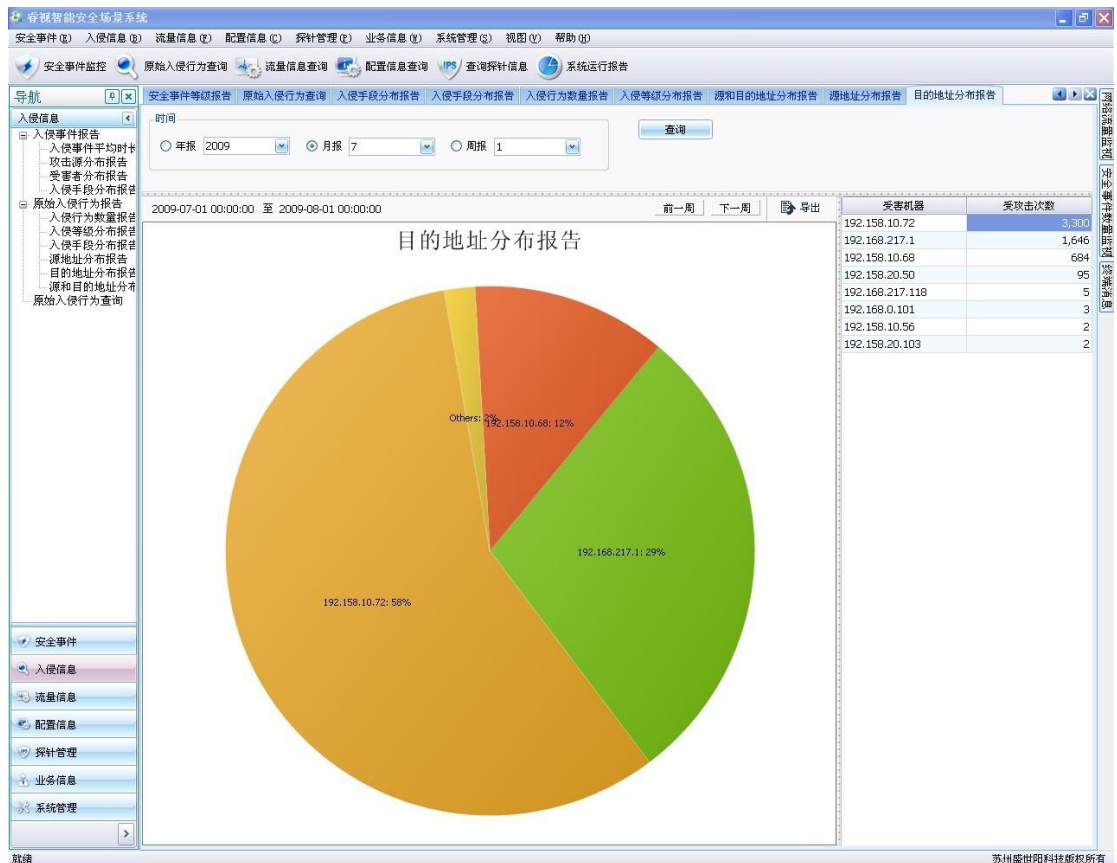


图 7-26 入侵行为目的地址统计报表

6.15. 查询流量信息

6.15.1 描述

输入多个查询条件，根据查询条件检索出符合条件的网络流量信息，并可对查询结果中的流量信息列表进行进一步的操作（发送通知类消息、发送控制类消息、发送查询类消息、查看配置信息、查看设备信息、查看相关的安全事件）。

6.15.2 进入方式

- 1、菜单项：“流量信息” -> “流量信息查询”；
- 2、工具栏上点击“流量信息查询”按钮；
- 3、导航栏：“流量信息” -> “流量信息查询”。

6.15.3 操作步骤

- 1、在查询条件（详见输入数据）中输入要查询的内容（如果某个查询条件不输入内容，表示对该条件不作限制，初始状态下对所有条件不作限制），点击“确定”按钮；

2、系统以流量信息列表的形式给出查询结果。

6.15.4 相关操作

对于查询结果，可以通过右键菜单进行如下操作：

- 1、发送通知类消息，详见 7.3.13；
- 2、发送控制类消息，详见 7.3.14；
- 3、查看运行状态，详见 7.3.16；
- 4、查看配置信息，详见 7.3.17；
- 5、查看设备信息，详见 7.3.18；
- 6、查看流量信息，详见 7.3.19
- 7、查看相关的安全事件，详见 7.3.20。

6.15.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.15.6 输入数据

名称	说明	输入举例
设备编号	流量信息相关的设备的编号	
设备类型	流量信息相关的设备的类型（主机、服务器）	全部
设备名称	流量信息相关的设备的名称	
等级	流量信息相关的设备的等级（高、中、低）	全部
所属部门	流量信息相关的设备的所属部门	
责任人	流量信息相关的设备的责任人	
IP 地址	流量信息相关的设备的 IP 地址	192.158.10.72
时间范围	包括起始时间和结束时间，在该时间范围内的流量信息才是符合查询条件的，该查询条件必须被输入	从 2009-8-4 到 2009-8-5
周期	流量数据的采样周期（15 分钟或 24 小时）	15 分钟

表格 6-23 查询流量信息输入数据表

6.15.7 输出数据

名称	说明	输出举例
IP 地址	流量信息相关的设备的 IP 地址	192.158.10.72
起始时间	采集流量信息的起始时间	2009-8-4 09:15:00
结束时间	采集流量信息的结束时间	2009-8-4 09:30:00
字节总数	一个设备在一段时间内的网络流量总字节数（以 KB 为单位）	33305
包总数	一个设备在一段时间内的网络流量数据包总数	31
TCP 字节数	网络流量中 TCP 协议相关的总字节数（以 B 为单位）	32305
UDP 字节数	网络流量中 UDP 协议相关的总字节数（以 B 为单位）	466
ICMP 字节数	网络流量中 ICMP 协议相关的总字节数（以 B 为单位）	2
ARP 字节数	网络流量中 ARP 协议相关的总字节数（以 B 为单位）	0
TCP 包数	网络流量中 TCP 协议相关的数据包总数	29
UDP 包数	网络流量中 UDP 协议相关的数据包总数	0
ICMP 包数	网络流量中 ICMP 协议相关的数据包总数	0
ARP 包数	网络流量中 ARP 协议相关的数据包总数	0

表格 6-24 查询流量信息输出数据表

6.15.8 操作举例

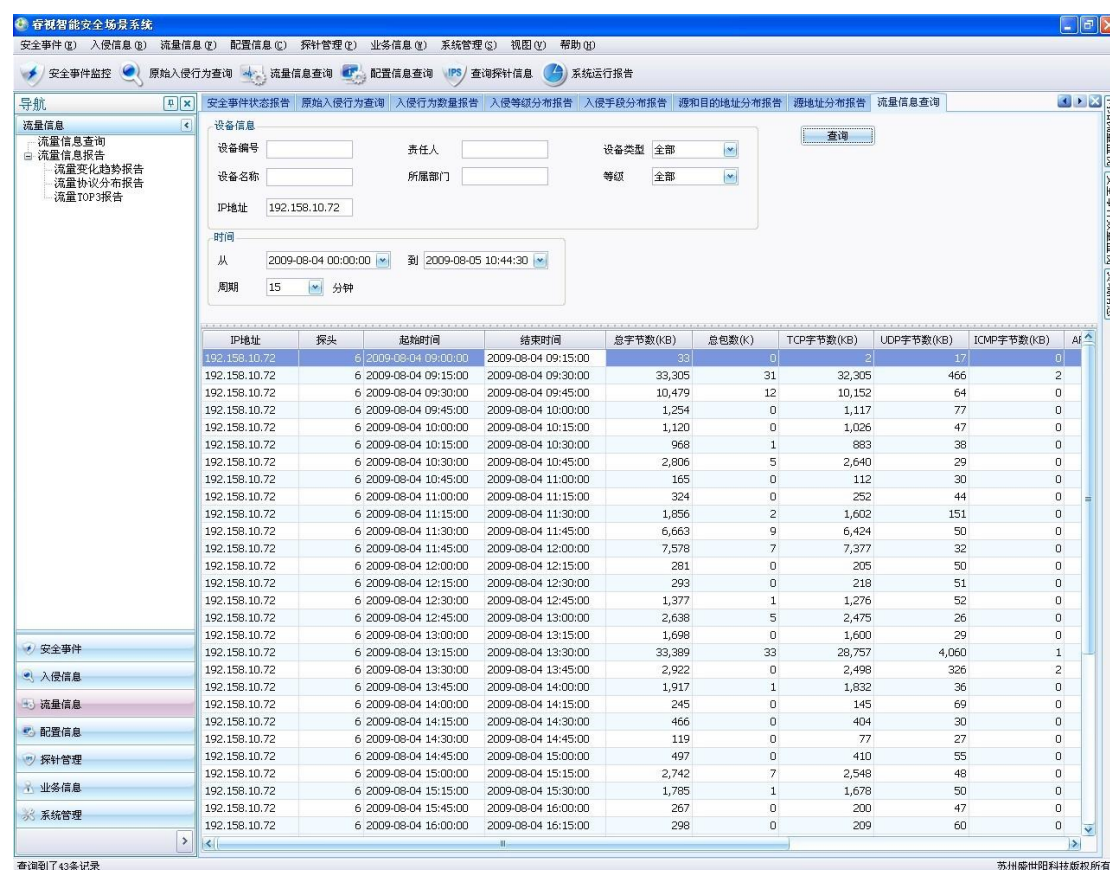


图 7-27 查询流量信息

6.16. 查看协议流量分布报告

6.16.1 描述

查看协议流量统计年报（指定的年中各个协议的网络流量和比例）、协议流量统计月报（指定的月中各个协议的网络流量和比例）、协议流量统计周报（指定的周中各个协议的网络流量和比例），以列表的形式给出给各个协议的网络流量，以饼图的形式给出各个协议的网络流量的比例。

6.16.2 进入方式

- 1、菜单项：“流量信息”->“流量信息报告”->“流量协议分布报告”；
- 2、导航栏：“流量信息”->“流量信息报告”->“流量协议分布报告”。

6.16.3 操作步骤

- 1、选择报表类型（年报/月报/周报）；

- 2、如果选中了年报，则必须输入具体的年；如果选中了月报，则必须输入具体的年和月；如果选中了周报，则必须输入具体的年、月和周；
- 3、选择统计单位（按字节数统计/按数据包数统计）；
- 4、如有需要，可以输入设备信息（详见输入数据）作为限制条件；
- 5、点击“确定”按钮；
- 6、系统以饼图和列表的形式给出报表。

6.16.4 相关操作

无

6.16.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.16.6 输入数据

名称	说明	输入举例
报表类型	报表的类型：年报、月报、周报	年报
年	某一年的年报或者是某年某月的月报或者是某年某月某周的周报	2009
月	某年某月的月报或者是某年某月某周的周报	7
周	查看周报时的某年某月的第几周	1
统计单位	根据字节数或数据包数进行统计	包数
设备编号	流量信息相关的设备的编号	
设备类型	流量信息相关的设备的类型（主机、服务器）	全部
设备名称	流量信息相关的设备的名称	
等级	流量信息相关的设备的等级（高、中、低）	全部
所属部门	流量信息相关的设备的所属部门	
责任人	流量信息相关的设备的责任人	
IP 地址	流量信息相关的设备的 IP 地址	192. 158. 10. 72

表格 6-25 协议流量统计报表输入数据表

6.16.7 输出数据

名称	说明	输出举例
协议	网络流量相关的网络协议	TCP
数量	某网络协议的网络流量（字节数或数据包数）	1041;89%

表格 6-26 协议流量统计报表输出数据表

6.16.8 操作举例

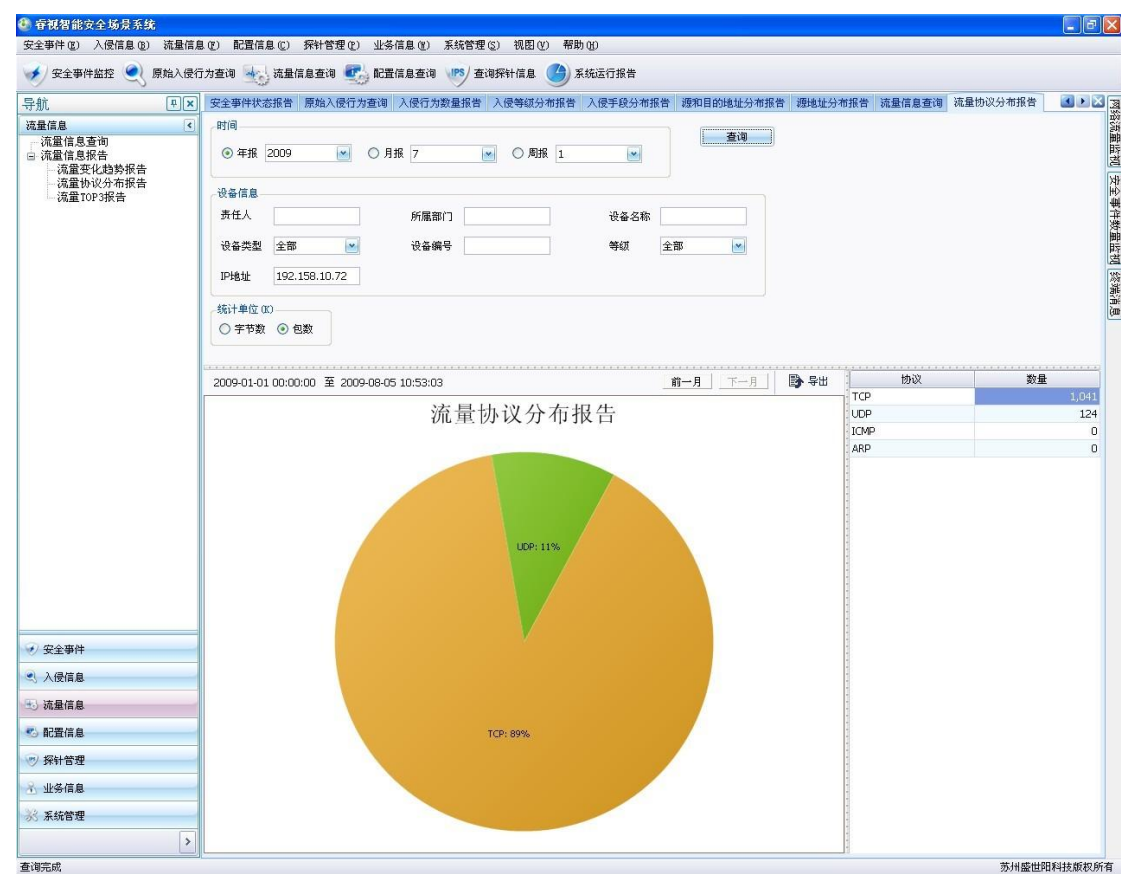


图 7-28 协议流量统计报表

6.17. 查看流量变化趋势报告

6.17.1 描述

查看某个 IP 地址的流量趋势年报（指定的年中该 IP 地址在每个月的网络流量，包括字节数和暑假包数）、流量趋势月报（指定的月中该 IP 地址在每个周的网络流量，包括字节数和暑假包数）、流量趋势周报（指定的周中该 IP 地址在每天的网络流量，包括字节数和暑假包数），以曲线图的形式展示。

6.17.2 进入方式

- 1、菜单项：“流量信息”->“流量信息报告”->“流量变化趋势报告”；
- 2、导航栏：“流量信息”->“流量信息报告”->“流量变化趋势报告”。

6.17.3 操作步骤

- 1、选择报表类型（年报/月报/周报）；
- 2、如果选中了年报，则必须输入具体的年；如果选中了月报，则必须输入具体的年和月；如果选中了周报，则必须输入具体的年、月和周；
- 3、输入 IP 地址（必须输入）；
- 4、点击“确定”按钮；
- 5、系统以曲线图的形式给出报表。

6.17.4 相关操作

无

6.17.5 异常处理

- 如出现查询失败的情况，请按如下步骤操作：
- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
 - 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.17.6 输入数据

名称	说明	输入举例
报表类型	报表的类型：年报、月报、周报	年报
年	某一年的年报或者是某年某月的月报或者是某年某月某周的周报	2008
月	某年某月的月报或者是某年某月某周的周报	7
周	查看周报时的某年某月的第几周	1
IP 地址	要查看流量趋势的设备的 IP 地址	192.158.10.142

表格 6-27 流量趋势报表输入数据表

6.17.7 输出数据

名称	说明	输出举例
柱状图横坐标	年报时为 1 月—12 月；月报时为第一周—第四周；周报时为该周的星期一—星期日	第一周、第二周、第三周、第四周
柱状图纵坐标	字节数（以 KB 为单位）、数据包数	107、19

表格 6-28 流量趋势报表输出数据表

6.17.8 操作举例

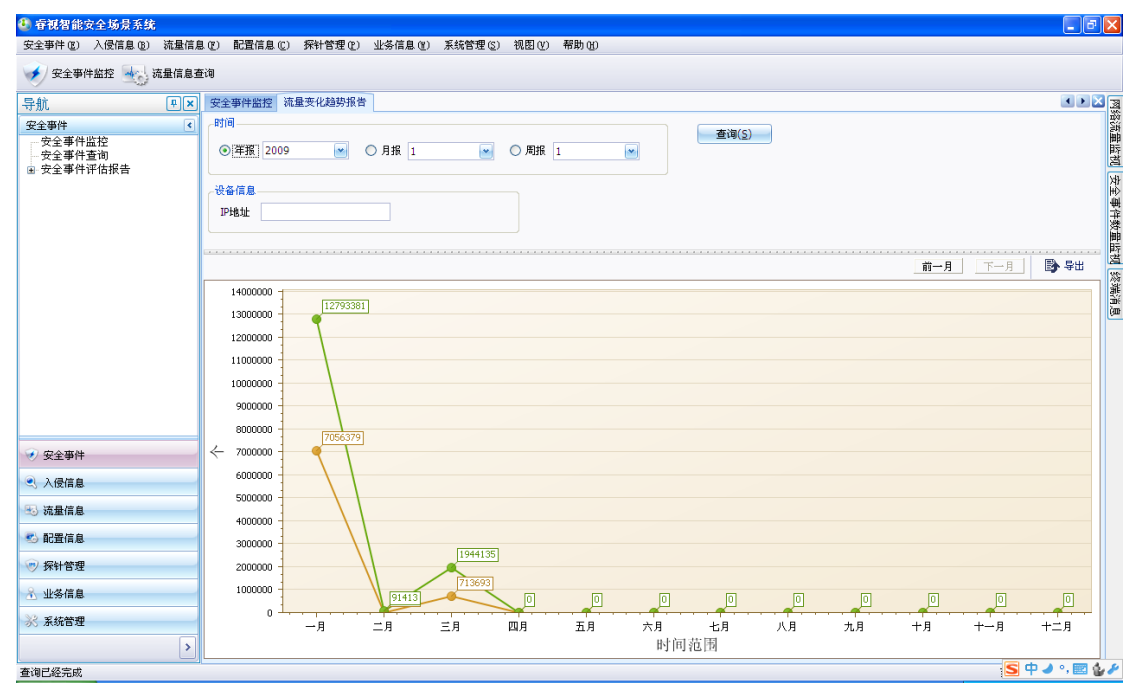


图 7-29 流量趋势统计报表

6.18. 查看流量 TOP3 报告

6.18.1 描述

查看各个 IP 地址在指定的时间范围内的网络流量和比例，以列表的形式给出给各个 IP 地址的网络流量，以饼图的形式给出各个 IP 地址的网络流量的比例（只列出比例前三名，三名之后的被累加为“其他”显示）。

6.18.2 进入方式

- 1、菜单项：“流量信息”->“流量信息报告”->“流量 TOP3 报告”；
- 2、导航栏：“流量信息”->“流量信息报告”->“流量 TOP3 报告”。

6.18.3 操作步骤

- 1、输入“起始时间”和“结束时间”（时间范围是必须输入的）；
- 2、选择统计单位（按字节数统计/按数据包数统计）；
- 3、如有需要，可以输入设备信息（详见输入数据）作为限制条件；
- 4、点击“确定”按钮；
- 5、系统以饼图和列表的形式给出报表。

6.18.4 相关操作

对于列表信息，可以通过右键菜单进行如下操作：

- 1、查看流量信息，详见 7.3.11；
- 2、查看相关的安全事件，详见 7.3.12。

6.18.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.18.6 输入数据

名称	说明	输入举例
起始时间（日期）	要评估的时间范围的起始时间的日期	2009-7-1
起始时间（时刻）	要评估的时间范围的起始时间的时刻	0:00:00
结束时间（日期）	要评估的时间范围的结束时间的日期	2009-8-5
结束时间（时刻）	要评估的时间范围的结束时间的时刻	11:00:00
统计单位	根据字节数或数据包数进行统计	字节数
设备类型	流量信息相关的设备的类型（主机、服务器）	全部
设备名称	流量信息相关的设备的名称	
等级	流量信息相关的设备的等级（高、中、低）	全部
所属部门	流量信息相关的设备的所属部门	

表格 6-29 流量评估报表输入数据表

6.18.7 输出数据

名称	说明	输出举例
IP 地址	被评估的 IP 地址	192.158.10.72
总数	某个 IP 地址的网络流量(字节数或数据包数)	1343191

表格 6-30 流量评估报表输出数据表

6.18.8 操作举例

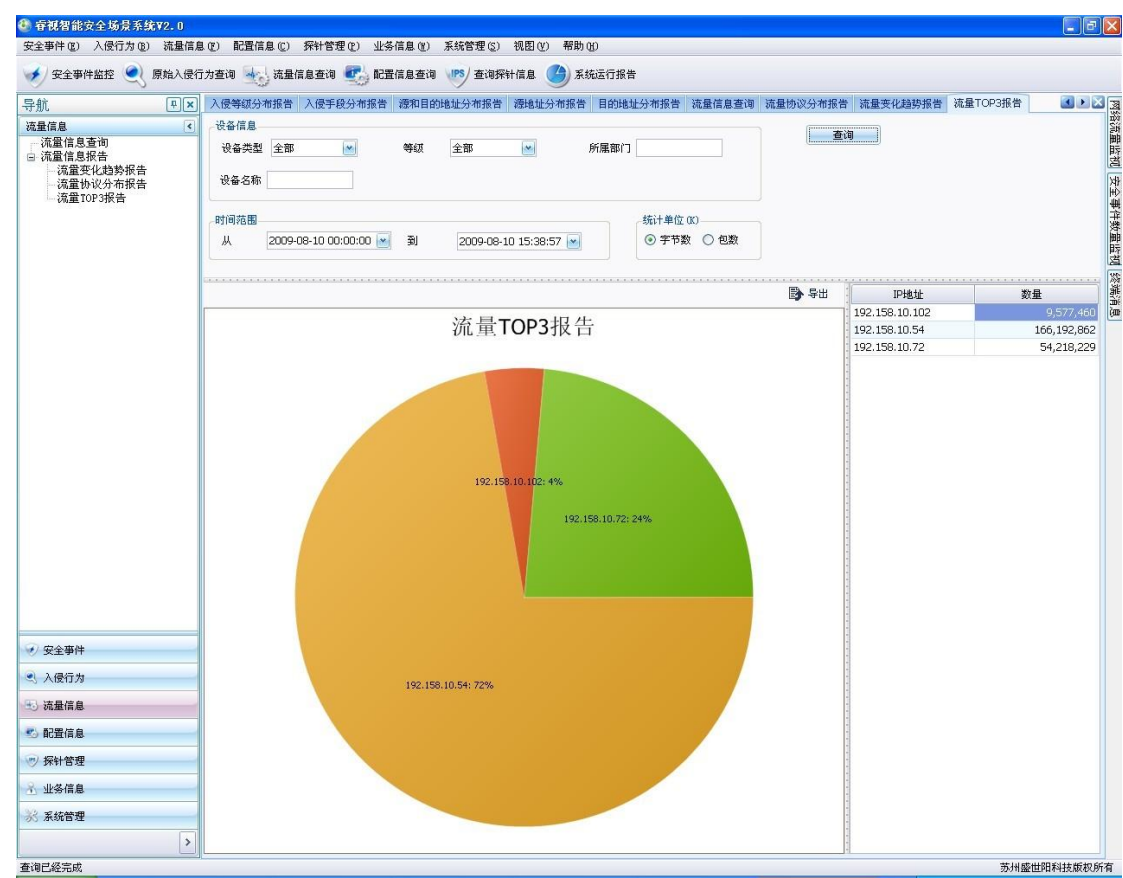


图 7-30 流量评估报表

6.19. 查看探针安装版本分布报告

6.19.1 描述

查看不同版本（软件版本或规则版本）的探针的比例，以饼图的形式展示（只列出比例前三名，三名之后的被累加为“其他”显示）。

6.19.2 进入方式

- 1、菜单项：“探针管理”->“探针信息报告”->“探针安装版本分布报告”；
- 2、导航栏：“探针管理”->“探针信息报告”->“探针安装版本分布报告”。

6.19.3 操作步骤

- 1、选择统计依据（探针软件版本/探针规则版本）；
- 2、点击“确定”按钮；
- 3、系统以饼图的形式给出报表。

6.19.4 相关操作

无

6.19.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.19.6 输入数据

名称	说明	输入举例
统计依据	根据探针软件版本或探针规则版本进行统计	探针软件版本

表格 6-31 探针版本统计报表输入数据表

6.19.7 输出数据

名称	说明	输出举例
版本	探针软件版本或探针规则版本	1. 2. 0. 1100
比例	某版本的探针在所有的安装的探针中的比例	17%

表格 6-32 探针版本统计报表输出数据表

6.19.8 操作举例

下图所示操作为：根据探针软件版本进行统计的版本统计报表。

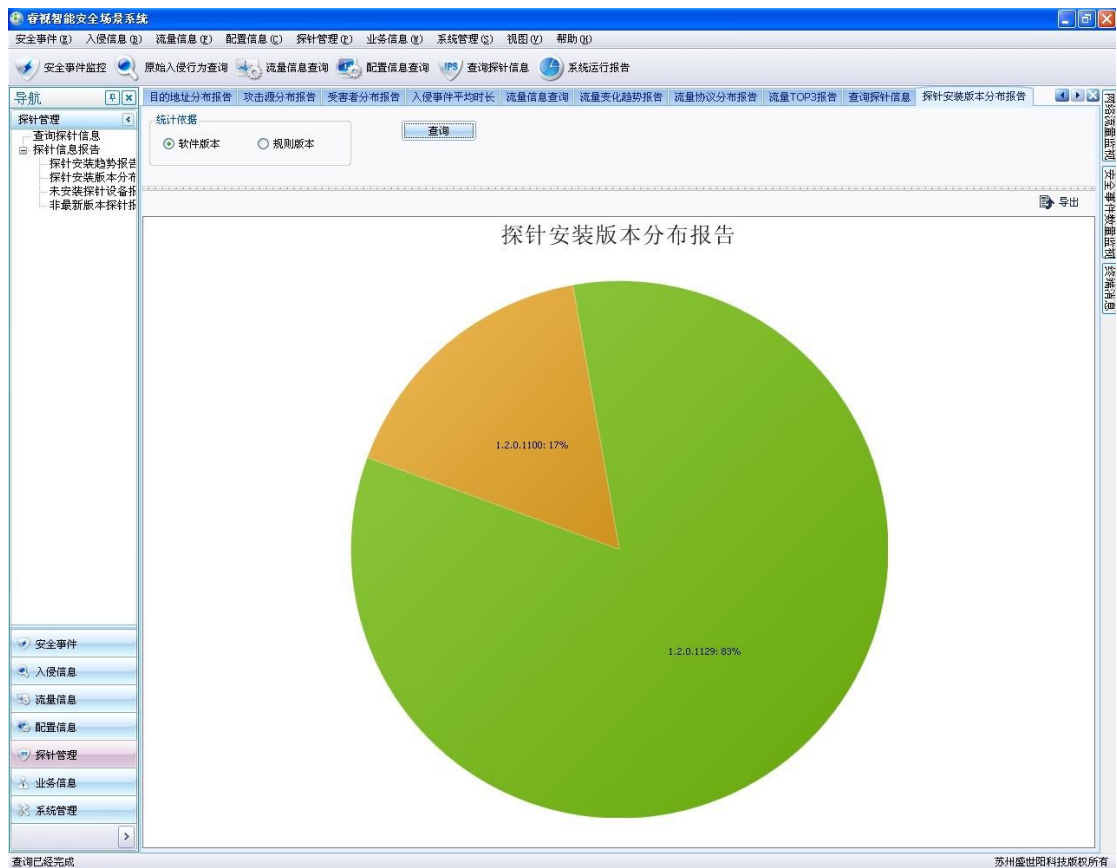


图 7-31 探针版本统计报表

6.20. 查看探针安装趋势报告

6.20.1 描述

查看探针安装趋势年报（指定的年中每个月的探针安装数量），月报（指定的月中每周的探针安装数量），周报（指定的周中每天的探针安装数量），以柱状图的形式展示报表。

6.20.2 进入方式

- 1、菜单项：“探针管理”->“探针信息报告”->“探针安装趋势报告”；
- 2、导航栏：“探针管理”->“探针信息报告”->“探针安装趋势报告”。

6.20.3 操作步骤

- 1、选择报表类型（年报/月报/周报）；
- 2、如果选中了年报，则必须输入具体的年；如果选中了月报，则必须输入具体的年和月；如果选中了周报，则必须输入具体的年、月和周；
- 3、点击“确定”按钮；

4、系统以柱状图的形式给出报表。

6.20.4 相关操作

无

6.20.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；

2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.20.6 输入数据

名称	说明	输入举例
报表类型	报表的类型：年报、月报、周报	年报
年	某一年的年报或者是某年某月的月报或者是某年某月某周的周报	2008
月	某年某月的月报或者是某年某月某周的周报	7
周	查看周报时的某年某月的第几周	1

表格 6-33 查看探针安装趋势报告输入数据表

6.20.7 输出数据

名称	说明	输出举例
柱状图横坐标	年报时为 1 月—12 月；月报时为第一周—第四周；周报时为该周的星期一—星期日	第一周、第二周、第三周、第四周
柱状图纵坐标	某月（周、天）中安装的探针数量	1453

表格 6-34 查看探针安装趋势报告输出数据表

6.20.8 操作举例

下图所示操作为：2009 年探针安装趋势年报。

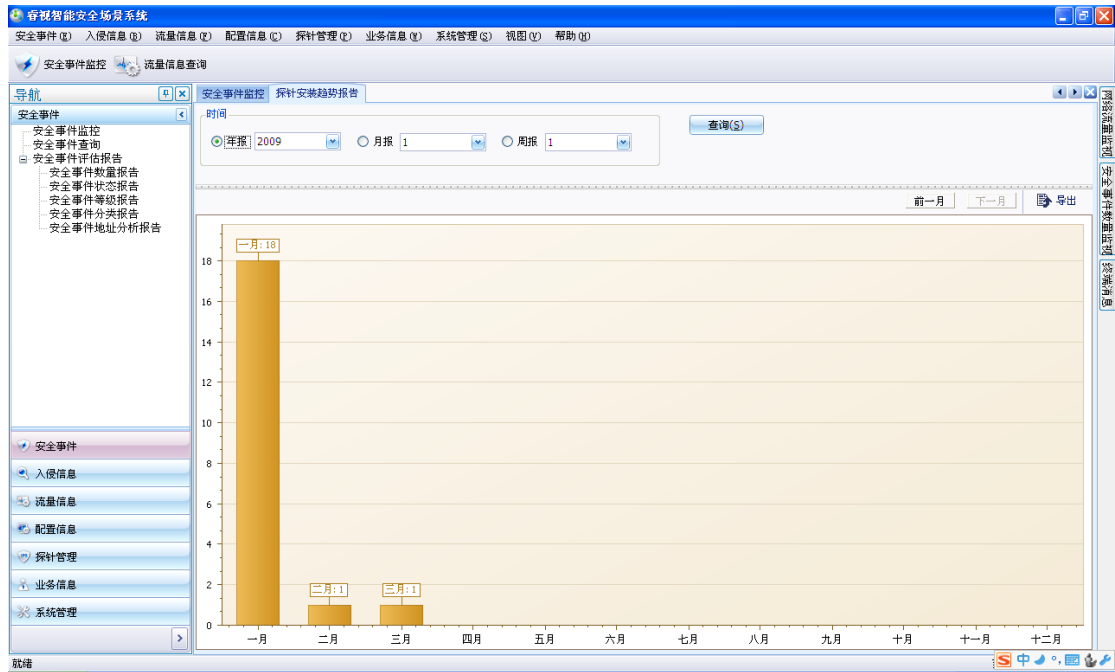


图 7-32 探针安装趋势报表

6.21. 查看未安装探针设备报告

6.21.1 描述

查看未安装探针的设备清单，以设备信息列表的形式展示。

6.21.2 进入方式

- 1、菜单项：“探针管理”->“探针信息报告”->“未安装探针设备报告”；
- 2、导航栏：“探针管理”->“探针信息报告”->“未安装探针设备报告”。

6.21.3 操作步骤

- 1、进入界面即得到未安装探针的设备清单。

6.21.4 相关操作

无

6.21.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.21.6 输入数据

无

6.21.7 输出数据

名称	说明	输出举例
编号	未安装探针的设备的编号	SSY-YF-200810-02
名称	未安装探针的设备的名称	研发用机
类型	未安装探针的设备的类型	主机
责任人	未安装探针的设备的责任人	李四

表格 6-35 未安装探针清单输出数据表

6.21.8 操作举例

下图所示操作为：查看未安装探针的设备清单。



图 7-33 探针安装评估报表

6.22. 查看非最新版本探针报告

6.22.1 描述

查看安装的不是最新版本的探针信息，以探针信息列表的形式展示。

6.22.2 进入方式

- 1、菜单项：“探针管理”->“探针信息报告”->“非最新版本探针报告”；
- 2、导航栏：“探针管理”->“探针信息报告”->“非最新版本探针报告”。

6.22.3 操作步骤

- 1、输入“最新软件版本”和“最新规则版本”（必须输入）；
- 2、点击“确定”按钮；
- 3、系统以列表的形式给出报表。

6.22.4 相关操作

无

6.22.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.22.6 输入数据

名称	说明	输入举例
最新软件版本	最新的软件版本	
最新规则版本	最新的知识库规则版本	

表格 6-36 非最新探针版本行为输入数据表

6.22.7 输出数据

名称	说明	输出举例
设备编号	安装非最新版本探针的设备的编号	SSY-fyw080014
设备名称	安装非最新版本探针的设备的名称	主机
设备类型	安装非最新版本探针的设备的类型	主机
责任人	安装非最新版本探针的设备的责任人	吴峰燕
软件版本	该设备上安装的探针软件版本	1.2.0.1100
规则版本	该设备上的探针知识库规则版本	alertbase.2.0.3.20090608

表格 6-37 非最新探针版本报告输出数据表

6.22.8 操作举例

下图所示操作为：查看非最新版本探针报告。

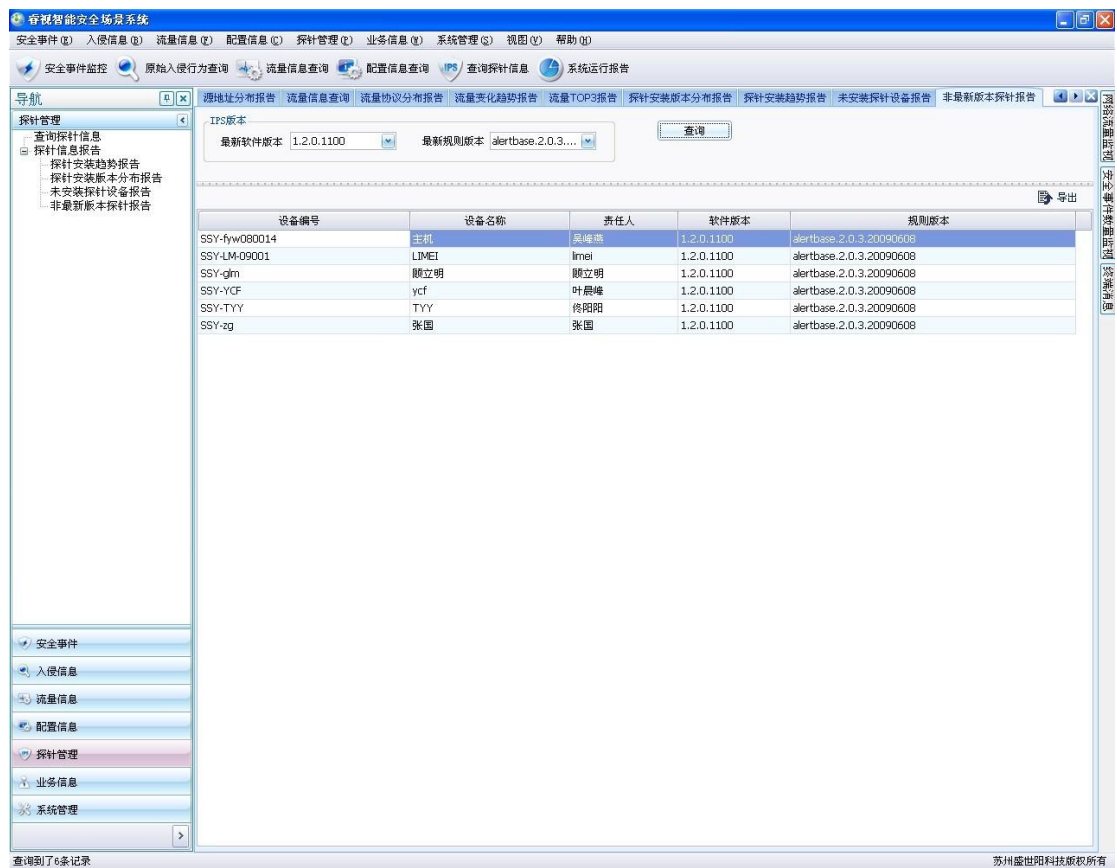


图 7-34 非最新版本探针报告

6.23. 查询探针信息

6.23.1 描述

输入多个查询条件，根据查询条件查询探针配置信息。

6.23.2 进入方式

- 1、菜单项：“探针管理”->“查询探针信息”；
- 2、导航栏：“探针管理”->“查询探针信息”。

6.23.3 操作步骤

- 1、在查询条件（详见输入数据）中输入要查询的内容（如果某个查询条件不输入内容，表示对该条件不作限制，初始状态下对所有条件不作限制），点击“确定”按钮；
- 2、系统以列表的形式给出查询结果。

6.23.4 相关操作

无

6.23.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.23.6 输入数据

名称	说明	输入举例
编号	设备的编号	
类型	设备的类型（主机、服务器）	全部
名称	设备的名称	
所属部门	设备的所属部门	
责任人	设备的责任人	
IP 地址	设备的 IP 地址	
软件版本	探针软件版本	
规则版本	探针知识库规则版本	

表格 6-38 查询探针配置信息输入数据表

6.23.7 输出数据

名称	说明	输出举例
设备编号		SSY-glm
设备名称		顾立明
设备类型	主机或服务器	主机
所属部门	设备的所属部门	insight
责任人	设备的责任人	顾立明
IP 地址	设备的 IP 地址	192.158.10.68
软件版本	该设备上安装的探针软件版本	1.2.0.1129
规则版本	该设备上的探针知识库规则版本	alertbase.2.0.3.20090608

表格 6-39 查询探针配置信息输出数据表

6.23.8 操作举例

下图所示操作为：

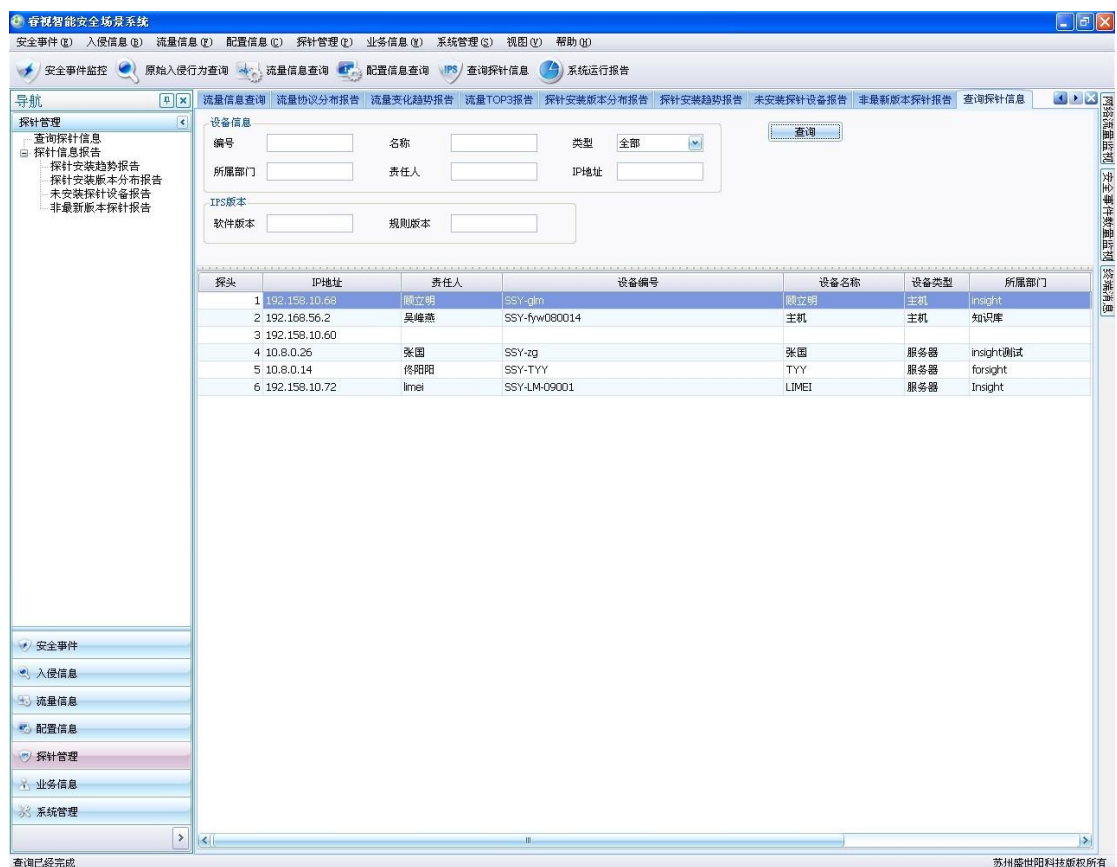


图 7-35 查询探针配置信息

6.24. 查询设备信息

6.24.1 描述

输入多个查询条件，根据查询条件检索出符合条件的设备信息。

6.24.2 进入方式

- 1、菜单项：“业务信息”->“设备管理”->“维护设备信息”；
- 2、导航栏：“业务信息”->“设备管理”->“维护设备信息”。

6.24.3 操作步骤

- 1、在查询条件（详见输入数据）中输入要查询的内容（如果某个查询条件不输入内容，表示对该条件不作限制，初始状态下对所有条件不作限制），点击“确定”按钮；
- 2、系统以列表的形式给出查询结果。

6.24.4 相关操作

可以对查询结果进行如下操作：

- 1、修改设备信息，详见 7.26;
- 2、删除设备信息，详见 7.27。

6.24.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.24.6 输入数据

名称	说明	输入举例
编号	设备的编号	SSY-YF-200810-01
类型	设备的类型（主机、服务器）	主机
名称	设备的名称	服务器
所属部门	设备的所属部门	IT 部
责任人	设备的责任人	张三
等级	设备的等级（高、中、低）	中
IP 地址	设备的 IP 地址	192. 168. 10. 142
安装日期	探针在设备上的安装日期	2008-10-20

表格 6-40 查询设备信息输入数据表

6.24.7 输出数据

名称	说明	输出举例
编号	设备的编号	SSY-YF-200810-01
类型	设备的类型（主机、服务器）	主机
名称	设备的名称	服务器
所属部门	设备的所属部门	IT 部
责任人	设备的责任人	张三
等级	设备的等级（高、中、低）	中
IP 地址	设备的 IP 地址	192. 168. 10. 142
安装日期	探针在设备上的安装日期	2008-10-20

表格 6-41 查询设备信息输出数据表

6.24.1 操作举例

下图所示操作为：查询全部类型全部等级的设备信息。

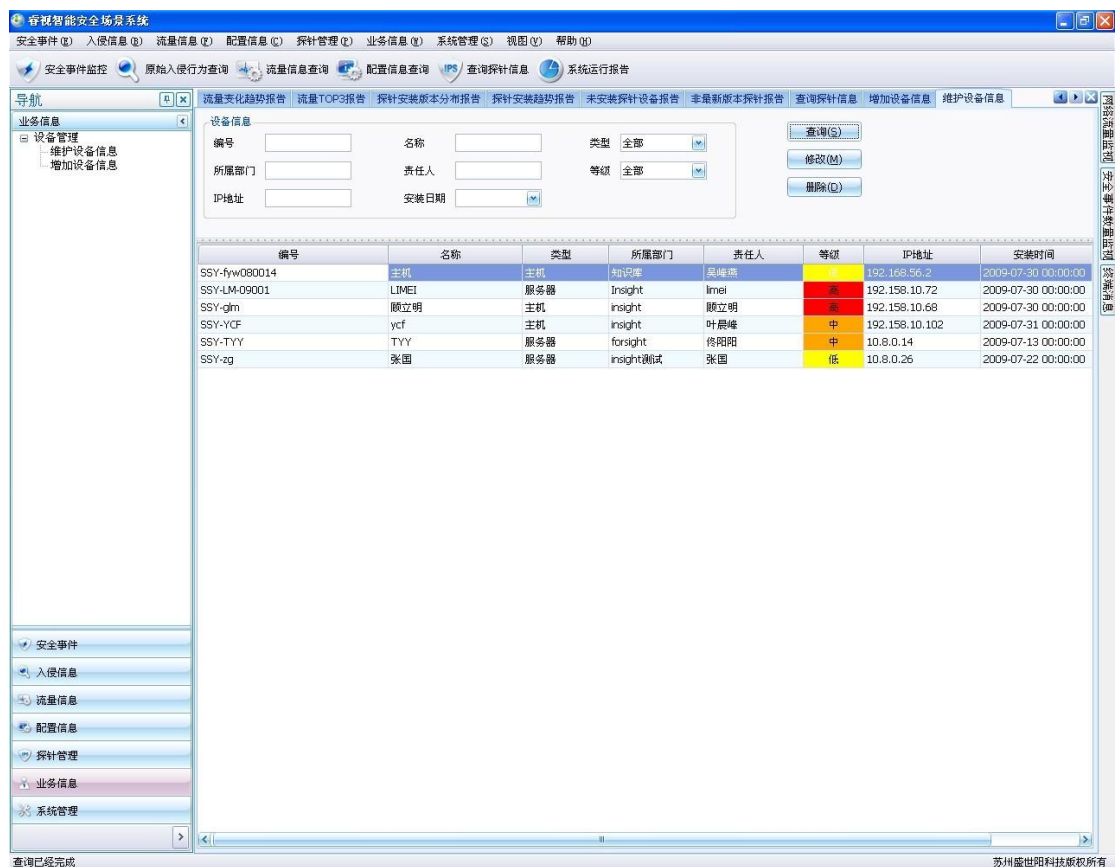


图 7-37 查询设备信息

6.25. 查询配置信息

6.25.1 描述

输入多个查询条件，根据查询条件检索出符合条件的设备的软硬件配置信息。

6.25.2 进入方式

- 1、菜单项：“配置信息”->“配置信息查询”；
- 2、导航栏：“配置信息”->“配置信息查询”。

6.25.3 操作步骤

- 1、在查询条件（详见输入数据）中输入要查询的内容（如果某个查询条件不输入内容，表示对该条件不作限制，初始状态下对所有条件不作限制），点击“确定”按钮；
- 2、系统以列表的形式给出查询结果。

6.25.4 相关操作

双击查询结果中的某一行，可以进行如下操作：

1、查看配置详细信息，详见 7.3.9。

6.25.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；

2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.25.6 输入数据

名称	说明	输入举例
编号	设备的编号	SSY-YF-200810-01
类型	设备的类型（主机、服务器）	主机
名称	设备的名称	服务器
等级	设备的等级（高、中、低）	中
所属部门	设备的所属部门	IT 部
责任人	设备的责任人	张三
IP 地址	设备的 IP 地址	192.168.10.142
操作系统名称	设备上安装的操作系统的名称	Microsoft Windows XP Professional
安装软件名称	设备上安装的软件之一的名称	Microsoft SQL Server
CPU 名称	设备的 CUP 的名称	Intel(R) Core(TM)2 CPU T7200 @ 2.00GHz
主板型号	设备的主板的型号	
网卡名称	设备的网卡的名称	Intel(R) PRO/Wireless 3945ABG Network Connection - Packet Scheduler Miniport

表格 6-42 查询配置信息输入数据表

6.25.7 输出数据

名称	说明	输出举例
设备编号		SSY-YF-200810-02
设备名称		研发用机
设备类型	主机或服务器	主机
所属部门	设备的所属部门	IT 部
责任人	设备的责任人	李四
IP 地址	设备的 IP 地址	192.158.10.142
操作系统	设备的操作系统的名称	Microsoft Windows XP SP2

主板型号	设备的主板型号	
内存容量	设备的内存的容量（单位 MB）	1536
硬盘容量	设备的硬盘的容量（单位 MB）	200054

表格 6-43 查询配置信息输出数据表

6.25.8 操作举例

下图所示操作为：查询所属部门是“insight”的全部设备的配置信息。

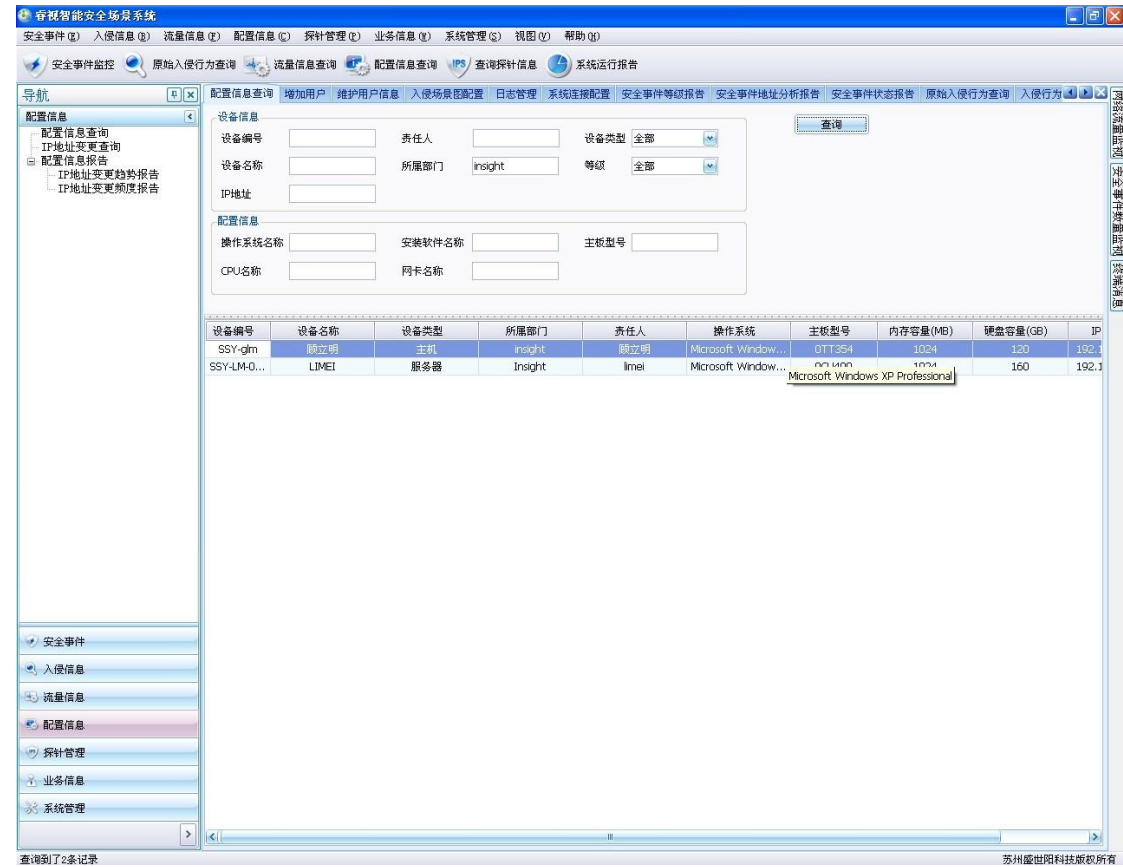


图 7-40 查询配置信息

6.26. IP 地址变更查询

6.26.1 描述

查看配置 IP 地址变更情况

6.26.2 进入方式

- 1、菜单项：“配置信息”->“IP 地址变更查询”；
- 2、导航栏：“配置信息”->“IP 地址变更查询”。

6.26.3 操作步骤

- 1、在查询条件（详见输入数据）中输入要查询的内容（如果某个查询条件不输入内容，表示对该条件不作限制，初始状态下对所有条件不作限制），点击“确定”按钮；
- 2、系统以列表的形式给出查询结果。

6.26.4 相关操作

无

6.26.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.26.6 输入数据

名称	说明	输入举例
编号	设备的编号	
类型	设备的类型（主机、服务器）	全部
名称	设备的名称	
所属部门	设备的所属部门	
责任人	设备的责任人	
时间范围	开始时间到结束时间	2009-7-26 到 2009-8-4

表格 6-44 配置变更报表输入数据表

6.26.7 输出数据

名称	说明	输出举例
资产类别	变更的配置的类别	IP 地址
变更情况	配置变更的情况	192.168.56.1 变为 192.168.56.2
变更时间	配置发生变更的时间	2009-8-3 09:06:00
设备编号		SSY-fyw080014
设备名称		主机
设备类型	主机或服务器	主机
所属部门	设备的所属部门	知识库
责任人	设备的责任人	吴峰燕

表格 6-45 配置变更报表输出数据表

6.26.8 操作举例

下图所示操作为：

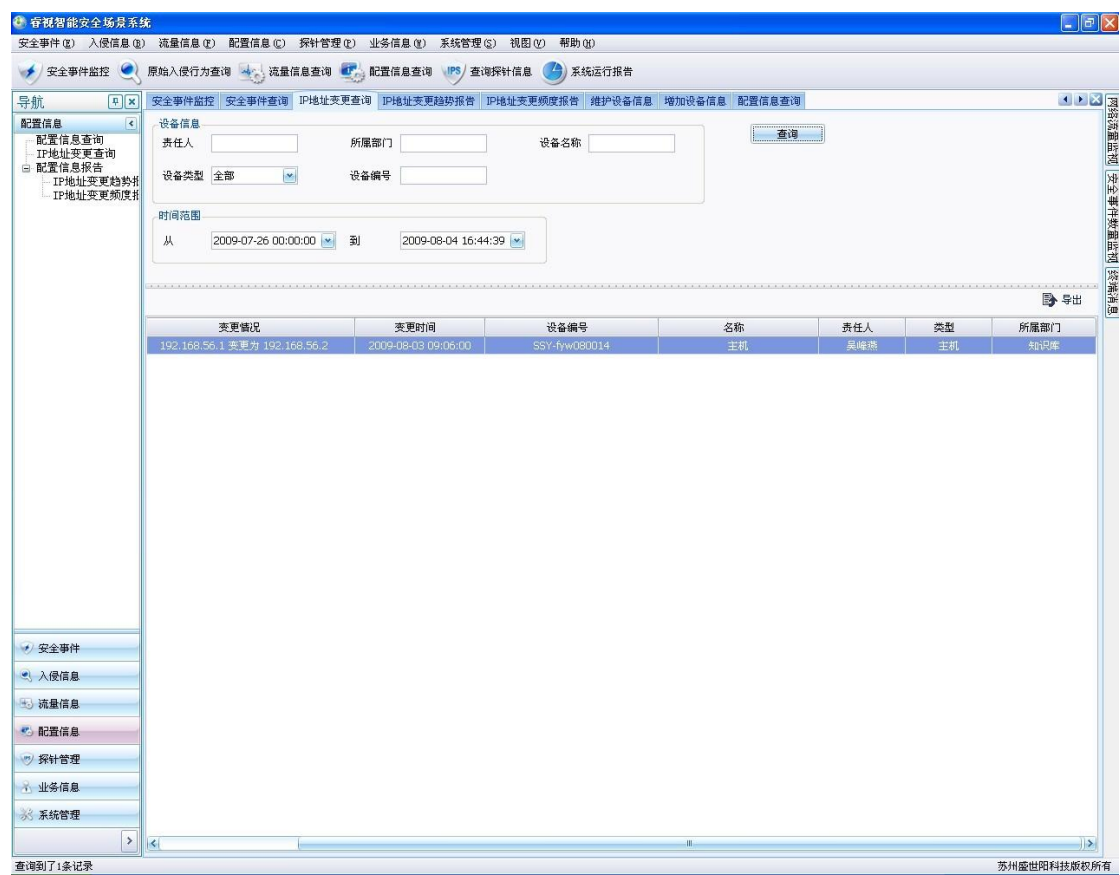


图 7-41 IP 地址变更报告

6.27. 查看 IP 地址变更频度报告

6.27.1 描述

查看某个终端设备的 IP 地址在某个时间段的变化平度，以列表的形式进行展示。

6.27.2 进入方式

- 1、菜单项：“配置信息”->“配置信息报告”->“IP 地址变更频度报告”；
- 2、导航栏：“配置信息”->“配置信息报告”->“IP 地址变更频度报告”。

6.27.3 操作步骤

- 1、在查询条件（详见输入数据）中输入要查询的内容（如果某个查询条件不输入内容，表示对该条件不作限制，初始状态下对所有条件不作限制），点击“确定”按钮；
- 2、系统以列表的形式给出报表。

6.27.4 相关操作

无

6.27.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.27.6 输入数据

名称	说明	输入举例
所属部门	设备的所属部门	IT 部
责任人	设备的责任人	张三
设备编号		SSY-YF-200810-01
设备类型	主机、服务器	主机
设备名称		财务专用机

表格 6-46 单终端 IP 地址变化频度报告输入数据表

6.27.7 输出数据

名称	说明	输出举例
设备编号		SSY-fyw080014
设备名称		主机
设备类型	主机或服务器	主机
所属部门	设备的所属部门	知识库
责任人	设备的责任人	吴峰燕
IP 地址		192. 168. 56. 2
变更次数		1

表格 6-47 单终端 IP 地址变化频度报告输出数据表

6.27.8 操作举例

下图所示操作为：

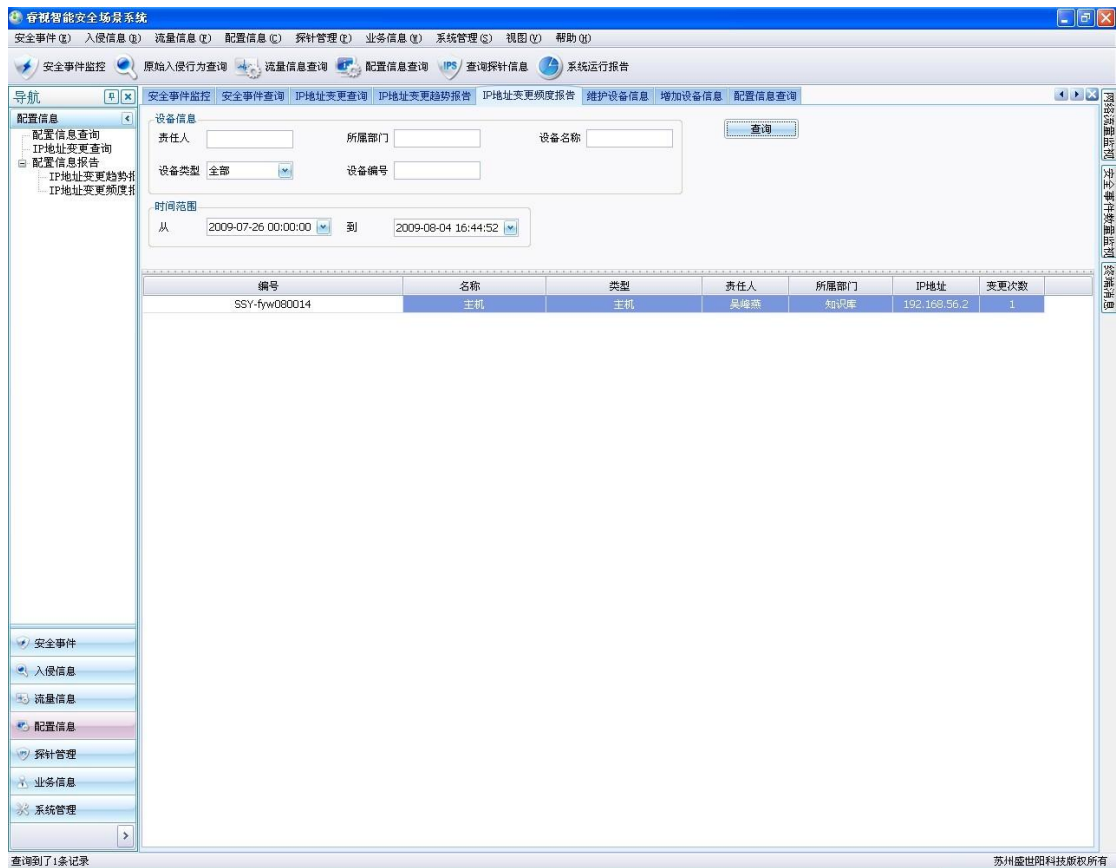


图 7-42 单终端 IP 地址变化频度报告

6.28. 查看 IP 地址变更趋势报告

6.28.1 描述

查看多个终端设备在指定的时间范围内的 IP 地址变化次数(变化次数为0的不会出现)，以信息列表的形式进行展示。

6.28.2 进入方式

- 1、菜单项：“配置信息”->“配置信息报告”->“IP 地址变更趋势报告”；
- 2、导航栏：“配置信息”->“配置信息报告”->“IP 地址变更趋势报告”。

6.28.3 操作步骤

- 2、在报表类型（年报/月报/周报）；
- 3、如果选中了年报，则必须输入具体的年；如果选中了月报，则必须输入具体的年和月；如果选中了周报，则必须输入具体的年、月和周；
- 4、如有需要，可以输入设备信息（详见输入数据）作为限制条件；

- 5、点击“查询”按钮；
- 6、显示查询结果

6.28.4 相关操作

无

6.28.5 异常处理

如出现查询失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.28.6 输入数据

名称	说明	输入举例
报表类型	报表的类型：年报、月报、周报	年报
年	某一年的年报或者是某年某月的月报或者是某年某月某周的周报	2009
月	某年某月的月报或者是某年某月某周的周报	7
周	查看周报时的某年某月的第几周	1
所属部门	设备的所属部门	
责任人	设备的责任人	
设备编号		
设备类型	主机、服务器	
设备名称		

表格 6-48 IP 地址变更趋势报告输入数据表

6.28.7 输出数据

名称	说明	输出举例
柱状图横坐标	年报时为 1 月—12 月；月报时为第一周—第四周；周报时为该周的星期一—星期日	2009 年一月到八月
柱状图纵坐标	某月/某周/某天的入侵行为数量	100

表格 6-49 IP 地址变更趋势报告输出数据表

6.28.8 操作举例

下图所示操作为：

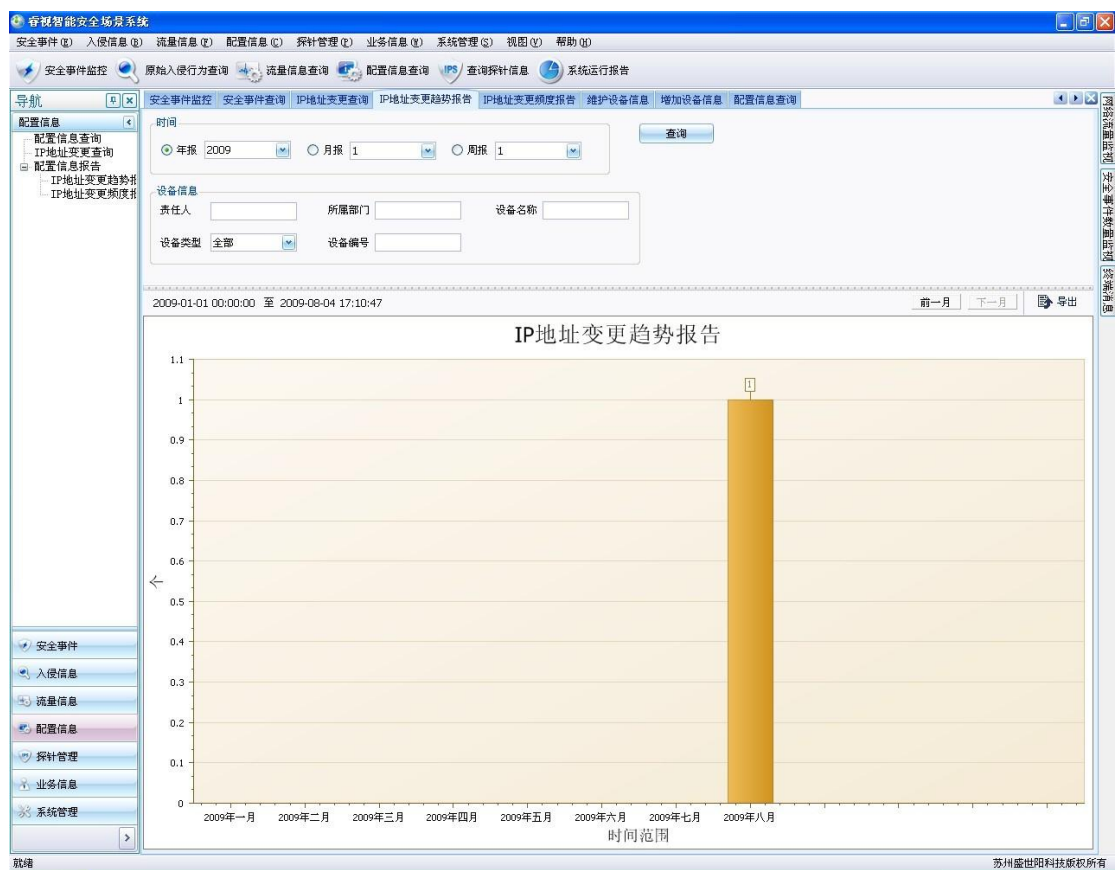


图 7-42 IP 地址变更趋势报告

6.29. 修改密码

6.29.1 描述

修改当前用户自己的密码。

6.29.2 进入方式

- 1、菜单项：“系统管理”->“修改密码”；
- 2、导航栏：“系统管理”->“修改密码”。

6.29.3 操作步骤

- 1、输入“原密码”；
- 2、输入“新密码”和“确认密码”（两者必须一样）；
- 3、点击“提交”按钮，确定进行修改。

6.29.4 相关操作

无

6.29.5 异常处理

如出现修改失败的情况，请按如下步骤操作：

- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
- 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.29.6 输入数据

名称	说明	输入举例
原密码	当前用户原来的密码	13457
新密码		Jlsh
确认密码	再次输入新密码进行验证	Jlsh

表格 6-50 修改密码输入数据表

6.29.7 输出数据

无

6.29.8 操作举例

下图所示操作为：修改密码。

修改密码

原密码

新密码

确认密码

提交(S)

取消(C)

图 7-44 修改密码

6.30. 网络流量监视

6.30.1 描述

可以实时查看当天网络流量前三名的信息。

6.30.2 进入方式

- 1、菜单项：“视图”->“流量 TOP3 监视”；
- 2、点击右侧边栏的“网络流量监视”。

6.30.3 操作步骤

打开界面即可看到当天网络流量前三名的信息。

6.30.4 相关操作

无

6.30.5 异常处理

无

6.30.6 输入数据

无

6.30.7 输出数据

名称	说明	输出举例
所属部门	设备的所属部门	IT 部
责任人	设备的责任人	张小非
IP 地址	流量信息相关的设备的 IP 地址	192. 168. 10. 142
总字节数	设备在当天的网络流量总字节数（以 KB 为单位）	31487
总包数	设备在当天的网络流量数据包总数	25

表格 6-51 网络流量监视输出数据表

6.30.8 操作举例

下图所示操作为：网络流量监视。

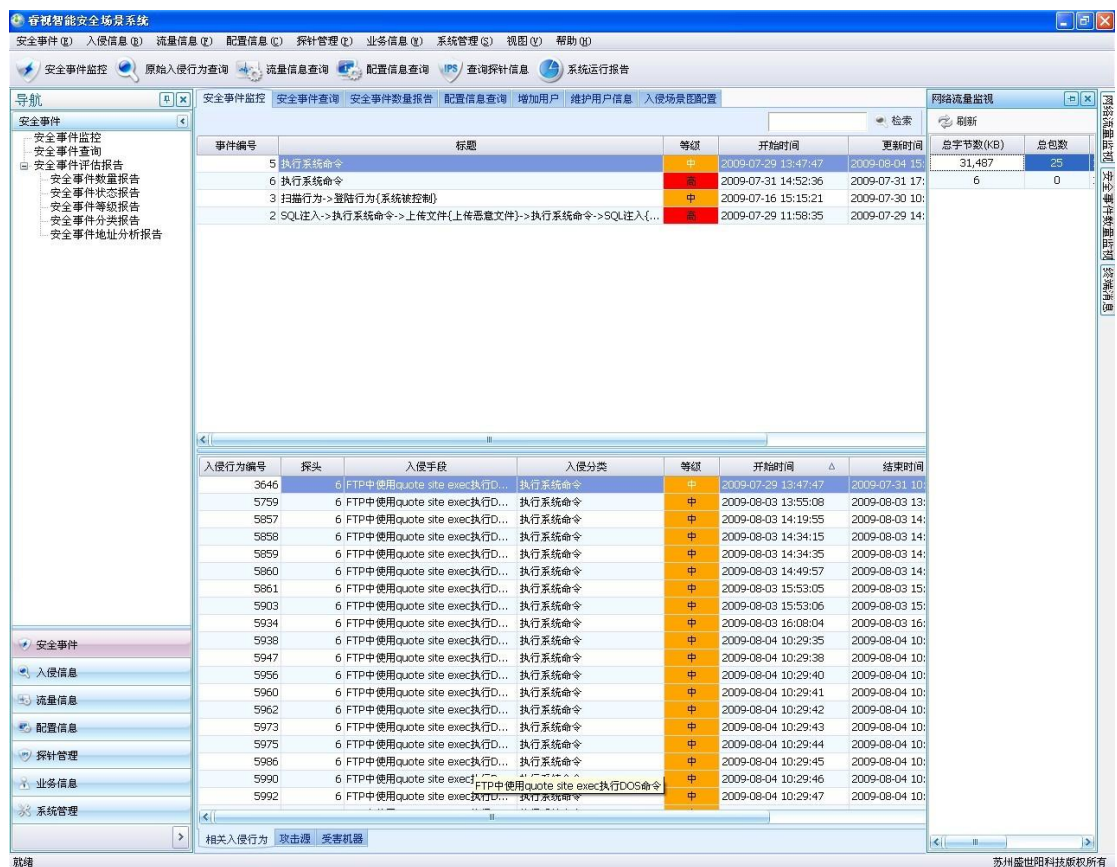


图 7-49 网络流量监视

6.31. 安全事件数量监视

6.31.1 描述

查看各个等级的安全事件的数量。

6.31.2 进入方式

- 1、菜单项：“视图”->“安全事件数量监控”；
- 2、点击右侧边栏的“安全事件数量监视”。

6.31.3 操作步骤

打开界面即可看到各个等级的安全事件的数量。

6.31.4 相关操作

无

6.31.5 异常处理

无

6.31.6 输入数据

无

6.31.7 输出数据

名称	说明	输出举例
等级	安全事件的等级（高、中、低）	高
新事件数量	未被确认和关闭的安全事件	0
已确认事件数量	已经被确认但还未关闭的安全事件	2

表格 6-52 安全事件数量监视输出数据表

6.31.8 操作举例

下图所示操作为：安全事件数量监视。



图 7-50 安全事件数量监视

6.32. 查看终端消息

6.32.1 描述

查看终端（安装有探针的设备）发送过来的消息。

6.32.2 进入方式

- 1、菜单项：“视图”->“响应消息监视”；
- 2、点击右侧边栏的“终端消息”。

6.32.3 操作步骤

打开界面即可看到终端发送过来的消息。

6.32.4 相关操作

无

6.32.5 异常处理

无

6.32.6 输入数据

无

6.32.7 输出数据

名称	说明	输出举例
终端消息	终端发送过来的消息，一般是通知类消息、控制类消息、查询类消息的反馈	接收到来自 192.158.10.72 的消息：通知类消息发送成功

表格 6-53 查看终端消息输出数据表

6.32.8 操作举例

下图所示操作为：查看终端消息。

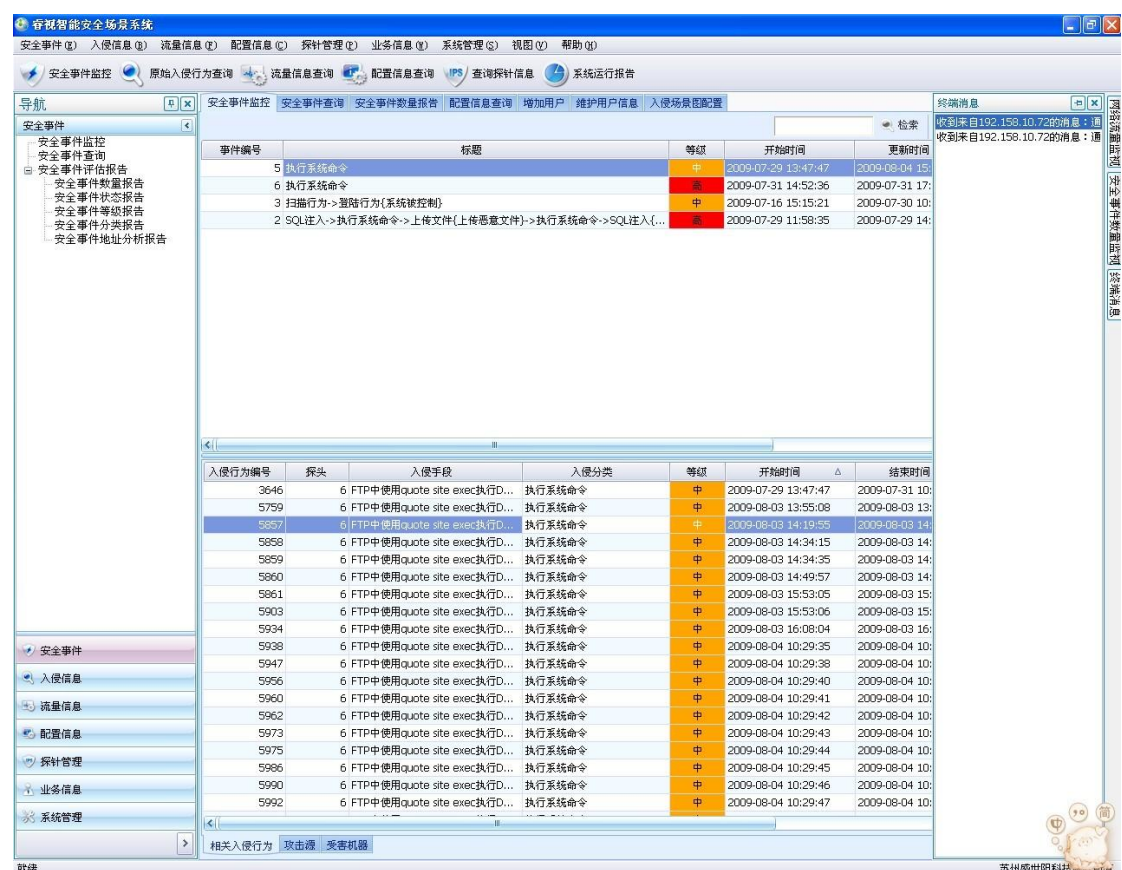


图 7-51 查看终端消息

6.33. 查询日志信息

6.33.1 描述

输入多个查询条件，根据查询条件检索出符合条件的系统日志信息。

6.33.2 进入方式

- 1、菜单项：“系统管理”->“日志管理”；
- 2、导航栏：“系统管理”->“日志管理”。

6.33.3 操作步骤

- 1、在查询条件（详见输入数据）中输入要查询的内容（如果某个查询条件不输入内容，表示对该条件不作限制，初始状态下对所有条件不作限制），点击“确定”按钮；
- 2、系统以列表的形式给出查询结果。

6.33.4 相关操作

可对日志中的某一条记录进行删除操作。

6.33.5 异常处理

- 如出现查询失败的情况，请按如下步骤操作：
- 1、检查管理端与服务端之间的网络连接是否正常，如正常则进入步骤 2，否则请联系相关人员恢复网络连接；
 - 2、请检查服务端是否正常运行（详见 6.1），如异常则重启服务端（详见 6.3）。

6.33.6 输入数据

名称	说明	输入举例
账号	日志记录的操作人员的账号	
内容	日志内容	
机器名	日志记录的机器名	
类型	日志的类型	
起始时间	待查询的时间段的起始时间	
结束时间	待查询的时间段的结束时间	

表格 6-54 查询日志信息输入数据表

6.33.7 输出数据

名称	说明	输出举例
账号	日志记录的操作人员的账号	
内容	日志内容	
机器名	日志记录的机器名	
类型	日志的类型	
时间	日志的记录时间	

表格 6-55 查询日志信息输出数据表

6.33.8 操作举例

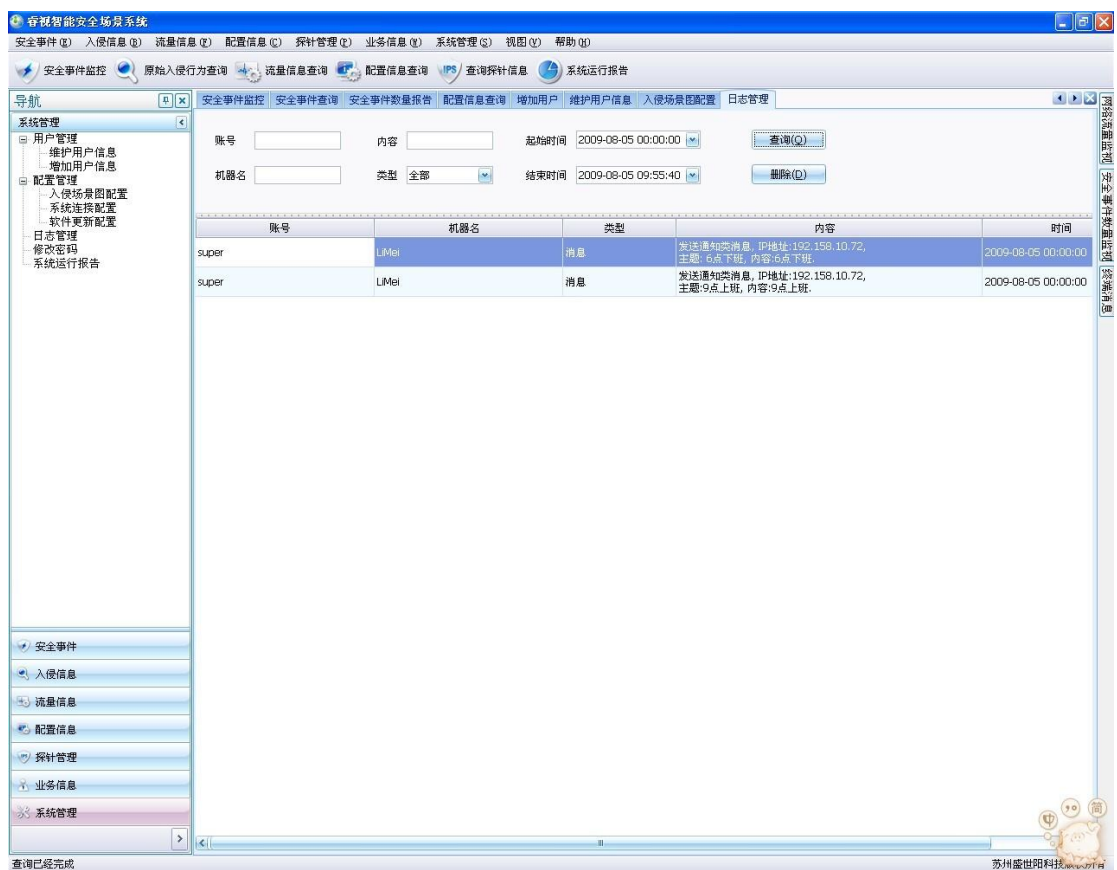


图 7-52 查询日志信息

6.34. 软件更新

6.34.1 描述

检查软件是否为最新版本，如果不是最新版本，则下载并安装最新版本。

6.34.2 进入方式

- 1、菜单项：“帮助”->“更新”。

6.34.3 操作步骤

- 1、如果检测到软件不是最新版本，系统弹出是否下载更新的对话框；
- 2、点击“是”按钮下载并安装最新版本，点击“否”取消更新。

6.34.4 相关操作

无

6.34.5 异常处理

网络连接故障

6.34.6 输入数据

无

6.34.7 输出数据

无

6.34.8 操作举例



图 7-53